Osgoode Hall Law Journal

Volume 58 | Issue 1 Article 1

3-9-2021

Voter Privacy and Big-Data Elections

Elizabeth F. Judge
Centre for Law, Technology and Society, Faculty of Law, University of Ottawa

Michael Pal
Centre for Law, Technology and Society, Faculty of Law, University of Ottawa

Voter Privacy and Big-Data Elections

Abstract

Big data and analytics have changed politics, with serious implications for the protection of personal privacy and for democracy. Political parties now hold large amounts of personal information about the individuals from whom they seek political contributions and, at election time, votes. This voter data is used for a variety of purposes, including voter contact and turnout, fundraising, honing of political messaging, and microtargeted communications designed specifically to appeal to small subsets of voters. Yet both privacy laws and election laws in Canada have failed to keep up with these developments in political campaigning and are in need of reform to protect voter privacy. We provide an overview of big data campaign practices, analyze the gaps in Canadian federal privacy and election law that enable such practices, and offer recommendations to amend federal laws to address the threats to voter privacy posed by big data campaigns.

1

Voter Privacy and Big-Data Elections

ELIZABETH F. JUDGE AND MICHAEL PAL*

Big data and analytics have changed politics, with serious implications for the protection of personal privacy and for democracy. Political parties now hold large amounts of personal information about the individuals from whom they seek political contributions and, at election time, votes. This voter data is used for a variety of purposes, including voter contact and turnout, fundraising, honing of political messaging, and microtargeted communications designed specifically to appeal to small subsets of voters. Yet both privacy laws and election laws in Canada have failed to keep up with these developments in political campaigning and are in need of reform to protect voter privacy. We provide an overview of big data campaign practices, analyze the gaps in Canadian federal privacy and election law that enable such practices, and offer recommendations to amend federal laws to address the threats to voter privacy posed by big data campaigns.

* Dr. Elizabeth F. Judge is Professor of Law and a member of the Centre for Law, Technology and Society at the Faculty of Law at the University of Ottawa in Ottawa, Canada. Dr. Michael Pal is an Associate Professor and a member of the Centre for Law, Technology and Society at the Faculty of Law at the University of Ottawa. We are grateful to the Social Sciences and Humanities Research Council of Canada for financial support for early research on this project awarded through a SSHRC Knowledge Synthesis Grant. Our KSG Report, "Privacy and the Electorate: Big Data and the Personalization of Politics," (2016) is available at <techlaw.uottawa.ca/sshrc-ksg-privacy-and-electorate>. We thank Amir M Korhani, PhD candidate at the University of Ottawa, for his outstanding research assistance and dedication to the project.

THIS ARTICLE ADDRESSES THE CHALLENGES for voter privacy posed by Canadian political parties' use of big data analytics.[1] Big data, consisting of mass data collection and algorithmic analysis, is an integral part of Canadian politics, as parties collect, store, and analyze voter data in an effort to run more effective campaigns. As Ira Rubinstein defines the term, big data "refers to novel ways in which organizations, including government and businesses, combine diverse digital datasets and then use statistics and other data mining techniques to extract from them both hidden information and surprising correlations."[2] With big data techniques, large datasets are analysed for patterns, data is matched to categorise people into discrete segments by shared characteristics, and people are profiled

1. Throughout the article, we use "voter" as a shorthand to refer to the individuals whose personal information is collected and used by political parties. We do recognise that some of these individuals may not have voted or registered to vote, but they are subjects of data collection by the parties and are at least potential voters. This category is broader than eligible voters, whom Elections Canada refers to as "electors."
2. The term "big data" has been attributed to a 2011 McKinsey report. James Manyika et al, "Big Data: The Next Frontier for Innovation, Competition, and Productivity" (1 May 2011), online: *McKinsey Global Institute* <www.mckinsey.com/business-functions/digital-mckinsey/our-insights/big-data-the-next-frontier-for-innovation>. See generally, Ira S Rubinstein, "Big Data: The End of Privacy or a New Beginning" (2013) 3 Intl Data Privacy L 74 at 76.

according to inferences based on data correlations. Applied to the election context, big data refers to the collection of large quantities of personal information about voters, the development of political party databases, and the use of a diverse set of technologies common in the private sector to analyze this information, including sophisticated algorithms, machine learning, and predictive analytics. Canada is no anomaly in this respect, as the use of big data in electoral campaigns is now widespread globally. In short, "[e]lections are becoming increasingly 'datified.'"[3]

The rise of big data has immense implications for individual privacy, given the vast amounts of personal data collected and the lack of transparency about its use.[4] The uses and potential abuses of big data in politics received global attention, with reverberations in Canada, in light of allegations that Facebook data about voters was misused in the United Kingdom's Brexit referendum and in the United States' 2016 presidential election. In these incidents, data about Facebook users travelled downstream to a campaign consultant specializing in psychographic profiling, without users' knowledge, and ended up in the hands of Cambridge Analytica, which specialises in big data analytics. The high-profile media coverage of Cambridge Analytica heightened public awareness of the

3. UK, Information Commissioner's Office, *Democracy Disrupted? Personal Information and Political Influence* (ICO, 2018) at 10 [ICO, *Democracy Disrupted*]; Jamie Bartlett, Josh Smith & Rose Acton, *The Future of Political Campaigning* (Demos, 2018) at 26. See also Robert Yablon, "Campaigns, Inc." (2018) 103 Minn L Rev 151; Jeff Chester & Kathryn C Montgomer, "The Role of Digital Marketing in Political Campaigns" (2017) 6 Internet Pol'y Rev 1; Zeynep Tufekci, "Engineering the Public: Big Data, Surveillance and Computational Politics" (2014) 19 First Monday, online: < firstmonday.org/article/view/4901/4097>.

4. On big data and privacy see generally, Anita L Allen, "Protecting One's Own Privacy in a Big Data Economy" (2016) 130 Harv L Rev 71; Julia Lane et al, eds, *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (Cambridge University Press, 2014); Omer Tene & Jules Polonetsky, "Big Data for All: Privacy and User Control in the Age of Analytics" (2013) 11 Nw Tech & Intell Prop 239; Kate Crawford & Jason Schultz, "Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms" (2014) 55 Boston College L Rev 93; Solon Barocas, "Big Data's End Run Around Procedural Privacy Protections" (2014) 57 Comm ACM 31; Cathy O'Neil, *Weapons of Math Destruction* (Broadway Books, 2017).

privacy and political implications of vast troves of personal information being accessed and interpreted for elections.[5]

Canadian election and privacy law, however, has failed to keep pace with this move to digital campaigning, with significant implications for voter privacy. Unlike private companies' collection and use of consumer data, which is subject to regulation under existing privacy legislation, political parties' collection and use of voter data is largely exempt from federal privacy legislation. Political parties are specifically excluded from the federal privacy legislation regulating the public sector, the *Privacy Act*,[6] and are not included in the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*), the federal privacy legislation regulating the private sector.[7] While election law has mechanisms to provide basic

---

5. See generally Office of the Privacy Commissioner of Canada, *Trust but Verify: Rebuilding Trust in the Digital Economy Through Effective, Independent Oversight*, *2018*, (Annual Report to Parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act) Catalogue No IP51-1E-PDF (2018) online (pdf): <www.priv.gc.ca/media/4831/ar_201718_eng.pdf> [OPC, *Trust but Verify*] (on the electoral data targeting by Cambridge Analytica based on Facebook data); House of Commons, Standing Committee on Access to Information, Privacy and Ethics, *Towards Privacy by Design: Review of the Personal Information Protection and Electronic Documents Act*, (February 2018) (Chair: Bob Zimmer), online (pdf): <www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9690701/ethirp12/ethirp12-e.pdf> [ETHI, *Towards Privacy by Design*]; House of Commons, Standing Committee on Access to Information, Privacy and Ethics, *Democracy Under Threat: Risks and Solutions in the Era of Disinformation and Data Monopoly* (December 2018) (Chair: Bob Zimmer), online (pdf): <www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP10242267/ethirp17/ethirp17-e.pdf> [ETHI, *Democracy Under Threat*]; UK, Digital, Culture, Media and Sport Committee, *Disinformation and 'Fake News': Interim Report* (Cm 363, 2017-19) at 26-28 [Digital, Culture, Media and Sport Committee, Disinformation and *'Fake News' Interim Report*]; UK, Information Commissioner's Office, *Investigation into the Use of Data Analytics in Political Campaigns* (Report to Parliament) (6 November 2018), online (pdf): < ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf> at 26-39 [ICO, *Investigation into the Use of Data Analytics in Political Campaigns*]; Office of the Privacy Commissioner of Canada & Office of the Information and Privacy Commissioner of British Columbia, *Joint Investigation of AggregateIQ Data Services Ltd. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner of Canada,* (PIPEDA Report of Findings) Catalogue No 2019-004 (November 2019), online: <www.priv.gc.ca/en/opc-actions-and-decisions/investiations/investigations-into-businesses/2019/pipeda-2019-004> [OPC and OIPC BC, *Joint Investigation of AggregateIQ Data Services*]; Office of the Information and Privacy Commissioner of British Columbia, *Full Disclosure: Political Parties, Campaign Data, and Voter Consent,* Investigation Report by Michael McEvoy, 2019 BCIPC 07 [McEvoy, *Full Disclosure*].
6. *Privacy Act,* RSC 1985, c P-21.
7. SC 2000, c 5 [*PIPEDA*].

information about individual voters to political parties through the National Register of Elections, it fails in any meaningful way to regulate mass voter data collection by parties. This gap in legal protection is striking because parties' growing reliance on voter data and the increasingly sophisticated techniques for analyzing it have dramatically heightened the potential privacy risks for voters.

This article focuses on the practices of federal political parties[8] with respect to collecting, storing, and using voters' personal information and argues that political parties, like commercial entities and government, should be subject to privacy regulations.[9] The use of personal data for political purposes is as susceptible to misuse as the use of personal data for commercial activities, but with consequences that reverberate beyond the marketplace and into the legitimacy of electoral outcomes. Protecting voter privacy is necessary to safeguard the privacy of voters *and* to safeguard the integrity of the electoral process. As the Information Commissioner's Office in the United Kingdom warned, "we are at risk of developing a system of voter surveillance by default," which "could have a damaging long-term effect on the fabric of our democracy and political life."[10] Political parties are an essential conduit for the "meaningful participation" of Canadians in elections and for democracy more generally in Canada.[11] Without adequate protections for voter privacy, however, the evolving

---

8. Political parties are heavily regulated entities under the *Canada Elections Act.* See SC 2000, c 9 [*CEA*]. They are defined in section 2 as: "an organization one of whose fundamental purposes is to participate in public affairs by endorsing one or more of its members as candidates and supporting their election." While parties remain private rather than public organizations, their inner workings and legal obligations are defined in detail by the *CEA,* as are those of their "candidates" and "electoral district associations." "Candidates" are individuals nominated by the political party to represent them in an electoral district and an "electoral district association" "means an association of members of a political party in an electoral district" (*ibid,* s 2, 71(1)). Other relevant regulated entities under the *CEA* include third parties, which are defined by section 349 to be "a person or a group, other than a candidate, registered party or electoral district association of a registered party." Third parties are often labour unions, corporations, and civil society groups, but can also be individuals. See generally, Michael Pal, "Is the Permanent Campaign the End of the Egalitarian Model of Elections?" in Richard Albert, Paul Daly & Vanessa MacDonnell, eds, *The Canadian Constitution in Transition* (University of Toronto Press, 2019) 338 at 347-49 (for a recent discussion of the changing role of third parties).
9. We focus in this article on the law related to political parties. We emphasize from the outset, however, that a comprehensive solution for voter privacy requires addressing other actors and Canadian privacy law more generally.
10. ICO, *Democracy Disrupted, supra* note 3 at 9. See also ICO, *Investigation Into the Use of Data Analytics in Political Campaigns*, *supra* note 5 at 19.
11. *Figueroa v Canada (AG),* 2003 SCC 37 at para 27 [*Figueroa*].

big data practices of parties threaten to undermine the relationship between them and the voters they seek to influence and, most importantly, to represent.[12]

In the wake of recent incidents highlighting mass data use by political parties and the corresponding data vulnerabilities for voters, several changes have been put forward in Canada, including amendments to federal election law in the *Elections Modernization Act* (*EMA*)[13] and a Parliamentary committee report proposing to make political parties subject to *PIPEDA*.[14] While these are positive steps, the proposals do not go far enough. *PIPEDA* is a poor model to adopt for political parties because it does not impose sufficient privacy obligations on the private sector that it already regulates. Indeed, *with* the "protection" of *PIPEDA*, Canadians are extensively tracked online and are vulnerable to data breaches and prolific data collection and analysis.[15] The *EMA* has the objective of addressing electoral digital threats but does not impose strong substantive limits on what parties can do with personal information held about voters. Legal reform, therefore, is still required. Reform should be done in a manner that respects the personal information of voters and the foundational democratic connection between them and political parties. To protect Canadians' personal information in the special context of elections, we recommend that new legal duties be imposed on political parties that limit their use of voters' personal information, while still ensuring that parties have enough information about voters to formulate public policy and

12. Much has been written on the broader implications for democracy of digital campaigning. See generally, Philip Howard, *New Media Campaigns and the Managed Citizen* (Cambridge University Press, 2006); Daniel Kreiss, *Prototype Politics: Technology-Intensive Campaigning and the Data of Democracy* (Oxford University Press, 2016); Cass R Sunstein, *#Republic: Divided Democracy in the Age of Social Media* (Princeton University Press, 2017); Colin J Bennett, "Trends in Voter Surveillance in Western Societies: Privacy Intrusions and Democratic Implications" (2015) 13 Surveillance & Soc'y 370; Damian Tambini, "Social Media Power and Election Legitimacy" in Damian Tambini & Martin Moore, eds, *Digital Dominance: The Power of Google, Amazon, Facebook, and Apple* (Oxford University Press, 2018) 265 at 289 (noting that "while social media still *in theory* offer new opportunities for democracy, the increasingly commercial and increasingly smart, data-driven social media may in the long term be on a collision course with the open, voluntary, equal public deliberation required by democracy") [Tambini, "Social Media Power and Election Legitimacy"]. For the Canadian context, see Kaija Belfry Munroe & HD Munroe, "Constituency Campaigning in the Age of Data" (2018) 51 Can J Pol Sci 135.
13. SC 2018, c 31 [*EMA*].
14. ETHI, *Towards Privacy by Design*, *supra* note 5.
15. There is a vast literature on digital privacy. See *e.g.* H Jeff Smith, Tamara Dinev & Heng Xu, "Information Privacy Research: An Interdisciplinary Review" (2011) 35 MIS Q 989; Daniel Solove, *The Digital Person: Technology and Privacy in the Information Age* (NYU Press, 2004); Information and Privacy Commissioner of Ontario, *Privacy by Design: The 7 Foundational Principles,* by Ann Cavoukian (Information and Privacy Commissioner of Ontario, 2009).

to communicate with voters who consent to their personal information being used by political parties. Ensuring that political parties are subject to meaningful privacy rules is of paramount importance given the widespread and rising use of intrusive big data techniques in Canadian politics.

This article illustrates how Canadian federal legislation facilitates big data practices in politics, has failed to keep up with evolutions in political practice, and is in need of reform. Following this introduction, Part I explains the current framework under elections law for political parties to obtain data about voters, and details how Canadian political parties augment this information by recourse to big data. Part II explains the gaps in existing federal privacy and elections legislation (*PIPEDA*,[16] the *Privacy Act*,[17] and the *Canada Elections Act* (*CEA*),[18] including the 2018 amendments of the *EMA*[19]) and other relevant legislation, and examines the negative consequences for voter privacy of the legislative gaps. Part III advances a legal framework for enhancing voter privacy while still facilitating necessary communication between political parties and voters.

I. THE DATA PRACTICES OF CANADIAN PARTIES

Digital campaigns comprise a series of steps from identifying, learning about, and categorizing voters, to honing messages and communicating with them.[20] In federal politics in Canada, the process of voter data procurement begins with the *CEA*, which regulates political parties and other political entities. Under the *CEA*, parties are entitled to receive basic information about voters, which becomes the building block for data-led campaigning. Pursuant to section 44(1), the Chief Electoral Officer (CEO) maintains a National Register of Electors (the "Register"). The Register contains personal information about electors, consisting of the surname, given name, gender, date of birth, and civic and mailing addresses of each elector.[21] The definition for "personal information" in section 2(1) of the

16. *PIPEDA*, *supra* note 7.
17. *Privacy Act*, *supra* note 6.
18. *CEA, supra* note 8.
19. *EMA, supra* note 13.
20. See Tambini, "Social Media Power and Election Legitimacy," *supra* note 12, at 274 (on the generic stages of a social media political campaign). He identifies the stages as building the audience, audience segmentation, message creation and testing, message targeting, and delivery.
21. Elections Canada, "Description of the National Register of Electors" (2019), online: Elections Canada <www.elections.ca/content.aspx?section=vot&dir=reg/des&document=index&lang=e>.

CEA is the same as the one used in section 3 of the *Privacy Act*.[22] The accuracy of the information is enhanced via sharing agreements between federal and provincial bodies.[23] The Register serves to produce a list of electors to Elections Canada in order to administer the election,[24] and to Members of Parliament (MPs) and registered parties and their candidates in order to campaign.[25] Not all of the information is shared with political parties; for example, sex and date of birth are omitted.[26] Electors can choose to opt out of the Register[27] and to request access to the information that Elections Canada holds on them. The Privacy Commissioner may, at any time, audit how the personal information on the Register is protected.[28]

Candidates and MPs may use the list of electors to communicate with voters, including for the purposes of soliciting contributions and recruiting party members.[29] The 2014 amendments to the *CEA* in the *Fair Elections Act* (*FEA*)[30] increased the available voter data by granting political parties easier access to information about who has cast a ballot. These so-called "bingo cards" record the identification number for each person who votes and are shared daily during advance voting and more frequently on election day.[31]

---

22. *CEA*, *supra* note 8, s 2(1); *Privacy Act*, *supra* note 6, s 3.
23. *CEA*, *supra* note 8, s 55(2).
24. *Ibid*, ss 93, 104.1, 105, 107, 109. "Electors" is the term used by Elections Canada for eligible voters.
25. *Ibid*, s 45.
26. Elections Canada, "Guidelines on Use of the Lists of Electors" (September 2020), online: <www.elections.ca/content.aspx?section=pol&dir=ann/loe_guide&document=index&lang=e>.
27. Elections Canada, "Description of the National Register of Electors," *supra* note 21.
28. *Privacy Act*, *supra* note 6; see generally, Elections Canada, *supra* note 21.
29. *CEA*, *supra* note 8, ss 110, 111.
30. SC 2014, c 12 [*FEA*].
31. *Ibid*, s 52. This rule is now in section 291 of the *CEA*. See *CEA*, *supra* note 8, s 291. See also Laura Payton, "Privacy Concerns Raised by Marc Mayrand Over Election Changes," *Canadian Broadcasting Company* (6 March 2014), online: <www.cbc.ca/news/politics/privacy-concerns-raised-by-marc-mayrand-over-election-changes-1.2563048>; *Election Act*, RSBC, 1985, c A-1 [BC *EA*]. Similarly, in British Columbia, the provincial *Election Act* was amended to inform political parties who voted in the last provincial election. The Office of the Information and Privacy Commissioner for British Columbia called the amendment regrettable, partially due to the fact that the office lacked jurisdiction to enforce privacy protections against political parties. See Office of the Information and Privacy Commissioner for British Columbia, News Release, "Statement from B.C. Information and Privacy Commissioner regarding proposed amendments to Bill 20 (Election Amendment Act)" (14 May 2015), online (pdf): <www.oipc.bc.ca/news-releases/1792>. The British Columbia

To create more comprehensive voter profiles, political parties supplement basic voter data under the statutory entitlement with additional information from a variety of sources. Traditional means of acquiring voter data include telephone calls, door-to-door canvassing, surveys, polls, and records of political contributions.[32] Newer technologies for the collection of voter information, including mobile applications, social media, commercial data, and location tracking on mobile devices such as smartphones, have augmented these traditional mechanisms. The collated voter information is stored in voter management systems, commonly referred to as voter or political party databases.

While membership lists have long been kept by political parties, voter databases are a relatively new phenomenon.[33] The first Canadian political party to use a sophisticated database was the Conservative Party of Canada, whose Constituent Information Management System (CIMS) was built in 2004.[34] The Liberal Party of Canada built their own voter database management system called the "Liberalist."[35] The New Democratic Party currently uses a system called "Populus,"[36] replacing their old "NDP Vote" system.[37] The Green Party uses "Nation Builder," a commercially available application for voter management and community mobilization.[38] Apps for mobile devices enable canvassers to transfer information collected in the field to the central database.[39] Data for national and local campaigns are now generally linked. Data may also flow

---

Election Act does have some protections for voter privacy that are not present in the federal or other provincial statutes. See BC *EA, supra* note 31, s 275.

32. See Colin J Bennett & Robin M Bayley, *Canadian Federal Political Parties and Personal Privacy Protection: A Comparative Analysis* (Linden Consulting, 2012) online (pdf): *Office of the Privacy Commissioner of Canada* <www.priv.gc.ca/media/1756/pp_201203_e.pdf> at 16 [Bennet & Bayley, *Canadian Federal Political Parties and Personal Privacy*].
33. See Colin J Bennett, "The Politics of Privacy and the Privacy of Politics: Parties, Elections and Voter Surveillance in Western Democracies" (2013) 18 First Monday, online: <firstmonday.org/ojs/index.php/fm/article/view/4789/3730>.
34. Conservative Party of Canada database, "Constituent Information Management System," online: <www.apps.conservative.ca/login?rdr=https%3A%2F%2Fsupport.conservative.ca>.
35. Liberal Party of Canada database, "Liberalist," online: <www.liberalist.liberal.ca>.
36. New Democratic Party of Canada database, "Populus," online: <populus.ndp.ca/foreAction1/login/auth>.
37. See Susan Delacourt, *Shopping for Votes: How Politicians Choose Us and We Choose Them*, 2nd ed (Douglas and McIntyre, 2013) at 307; Colin Bennett, "They're Spying on You: How Party Databases Put Your Privacy at Risk" (1 September 2015), online: *iPolitics*, <ipolitics.ca/2015/09/01/theyre-spying-on-you-how- party-databases-put-your-privacy-at-risk>.
38. Nationbuilder, "Home," online: <www.nationbuilder.com>; McEvoy, *Full Disclosure*, *supra* note 5 at 27.
39. See *e.g.* Liberalist, "What is Liberalist," online: <www.liberalist.liberal.ca/what-is>.

between affiliated federal and provincial parties or between the national and provincial wings of a federal party. In some instances, provincial and federal databases are amalgamated, and in other instances provincial parties prefer to act independently of their federal counterparts' data strategies.[40] Provincial parties sometimes voluntarily subscribe to federal party databases.[41]

With the traditional techniques to collect information about voters, such as canvassing households, voters generally had the autonomy to choose whether to share information with parties and could vary the level of detail and the type of information shared. Over the course of the last several elections in Canada, however, voter data collection and analysis techniques have evolved rapidly such that data collection is less transparent and more intrusive.[42] In the absence of strong regulatory oversight from any level of government, it was difficult to know precisely the type and amount of personal information that each party collects, since parties typically viewed their data practices as providing a potential competitive advantage and were reticent about the sources and types of information collected.[43] However, investigations that were conducted globally by privacy commissioners in search of answers, after such high-profile voter data incidents as Cambridge Analytica, have revealed many details about parties' heretofore guarded practices surrounding data-driven campaigns.[44] Major technology-driven changes include parties' development of their own mobile apps, reliance on advertising through social media, use of databrokers as information intermediaries, reliance on predictive analyses, the application of big data analysis to discern information about segments of populations as well as individual voters, and the deployment of campaign strategies that borrow

40. Belfry Munroe & Munroe, *supra* note 12 at 16-18.
41. See Adrian Morrow, "Ontario Liberals to Target Ethnic Voters with Demographic Database Software" *The Globe and Mail* (14 April 2014), online: <www.theglobeandmail.com/news/politics/database-helps-liberals-woo-ethnic-vote/article17953049/>.
42. See Rebecca Green, "Petitions, Privacy, and Political Obscurity" (2013) 85 Temp L Rev 367 at 383; Philip N Howard & Daniel Kreiss, "Political Parties and Voter Privacy: Australia, Canada, the United Kingdom and United States in Comparative Perspective," (2010) 15 First Monday, online: <www.firstmonday.org/article/view/2975/2627>.
43. Bennett & Bayley, *Canadian Federal Political Parties and Personal Privacy Protection*, *supra* note 32 at 16; Howard & Kreiss, *supra* note 42 at 19.
44. OPC, *Trust but Verify*, *supra* note 5; ETHI, *Towards Privacy by Design*, *supra* note 5; ETHI, *Democracy Under Threat*, *supra* note 5; ICO, *Investigation into the Use of Data Analytics in Political Campaigns*, *supra* note 5; OPC and OIPC BC, *Joint Investigation of AggregateIQ Data Services*, *supra* note 5; McEvoy, *Full Disclosure*, *supra* note 5.

techniques from commercial marketing.[45] The investigations have illuminated how modern information technologies can enable even a small databroker's activities to wreak "global and cascading privacy implications" that cross continents and involve the data of tens of millions people.[46]

With the rise of big data, political parties can harness voter data by greater orders of magnitude, and subsequently target voters with far greater precision.[47] Political parties increasingly rely on data that is not overtly "political," including commercial information, to glean insights about voters' political preferences.[48] Data about voters is an amalgamation of consumer data, basic electoral data, public records, internet browsing, search engine queries, social media postings, mailing lists, subscriptions and memberships, loyalty cards, credit card information, online purchases, and geolocation information from mobile devices, which is added to the voter information that parties have collected based on their interactions with voters and the data provided from the Voter Contact Registry (the "Registry").[49] With the increased use of wearable devices (such as fitness trackers), home assistants, home security cameras, smart televisions, gaming consoles, and other Internet of Things devices, data will become increasingly precise and profuse about specific individuals, including activities and movements. Traditional metrics about voters, such as neighbourhood, income, educational level, and ethnicity, are rudimentary in relation to the variety and amount of information that can be collected about individuals from online and networked sources and the detailed tools for profiling available with modern algorithmic technologies.

Parties seek to learn ever more detailed information about increasingly discrete segments of the population and then to microtarget those audiences through advertising or other communications, honed to appeal specifically to that small subset's preferences, rather than the population as a whole. These techniques of big data are used prolifically and with more sophistication in each election

45. See Claudio Feijóo, José-Luis Gómez-Barroso & Shivom Aggarwal, "Economics of Big Data" in Johannes M Bauer & Michael Latzer eds, *Handbook on the Economics of the Internet* (Edward Elgar, 2016); ICO, *Investigation Into the Use of Data Analytics in Political Campaigns*, *supra* note 5 at 18.
46. OPC & OIPC BC, *Joint Investigation of AggregateIQ Data Services*, *supra* note 5, "Conclusion"; see also McEvoy, *Full Disclosure*, *supra* note 5.
47. ICO, *Democracy Disrupted*, *supra* note 3 at 21.
48. For example, the US Republican Party began using consumer information to target voters in the 1980s. See Green, *supra* note 42 at 384.
49. See Elizabeth F Judge & Michael Pal, *Privacy and the Electorate: Big Data and the Personalization of Politics* (SSHRC Knowledge Synthesis Grant Report) (October 2016).

cycle.[50] Big data produces a large economic ecosystem in which multiple players are involved in the curation, analysis, and use of data.[51] Political parties work in advance with analytic companies to develop their respective voter models.[52]

Social media companies like Google, Twitter, and Facebook have played an increasingly influential role in the new era of data-driven campaigns, facilitating targeted advertising and making social media an indispensable part of modern-day campaigns.[53] Social media platforms not only generate information about individuals based on their online activities, but are also used by parties and candidates to communicate with individuals.[54] Social media supports microtargeting by enabling parties to choose the audience for a message, and which version of that message is sent. For example, with Facebook, political parties can choose "core audiences" (whereby an audience is manually selected for particular traits such as location, gender, age, or interests); "custom audiences" (whereby parties upload individuals' contact details and Facebook matches that with their data); and "lookalike audiences" (whereby Facebook sends the message to a dynamically changing set of Facebook users who have similar interests to the

50. Belfry Munroe & Munroe, *supra* note 12. The UK's Information Commissioner's Office notes that the "extent to which political parties use social media, data analytics, and micro-targeting techniques is—to a large extent—dependent on their size, resources, and reach into the electorate." See ICO, *Democracy Disrupted*, *supra* note 3 at 21.
51. Feijóo, Gómez-Barroso & Aggarwal, *supra* note 45 at 513-14.
52. ICO, *Democracy Disrupted*, *supra* note 3 at 27.
53. As of February 2018, "Facebook and Google have 60% of US digital ad spend and 20% of total global spend." See Digital, Culture, Media and Sport Committee, Disinformation and *'Fake News' Interim Report*, *supra* note 5 at para 87. See also Daniel Kreiss & Shannon C McGregor, "Technology Firms Shape Political Communication: The Work of Microsoft, Facebook, Twitter, and Google with Campaigns During the 2016 U.S. Presidential Cycle" (2018) 35 *Pol Comm* 155 (on the major internet platforms' role as active agents in the political process of shaping political communications). Tambini cautions against the consolidation and vertical integration of campaign services in one platform, noting Facebook is a "one-stop-shop for fundraising, recruitment, profiling, segmentation, message targeting, and delivery" and is also a foreign company for most of the globe. As Tambini flags, platform dominance could lead to unintentional or deliberate biases. See Tambini, "Social Media Power and Election Legitimacy," *supra* note 12 at 281-82.
54. See Sofia Grafanaki, "Autonomy Challenges in the Age of Big Data" (2017) 27 Fordham IP Media & Ent LJ 801 at 859-60; Cathy O'Neil, *Weapons of Math Destruction* (Broadway Books, 2017) at 180-84.

fixed custom audience).[55] Social media platforms also create a larger ecosystem of data about people. Through access to contact lists on mobile devices and social media, personal information is collected not only about the user but also about a user's friends and family, a practice that has become increasingly controversial because of the lack of transparency to the user and a lack of consent by the contacts.[56] For instance, in some campaign apps, users are asked to login using their email, phone number, or Facebook account, where the latter grants the candidate's campaign access to personal information available on Facebook as well as a list of their friends and family (who do not have the opportunity to consent).[57] Further, social media companies exchange data about their users prolifically with other internet companies.[58]

---

55. See Facebook, "Ad Audiences," online: <www.facebook.com/business/help/168922287067163>. Facebook has offered "value-based lookalike audiences" since 2017. Likewise, Google Ads supports audience targeting by demographics, custom audiences, and "similar audiences." See Google Ads Help, "Targeting Your Ads," online: <www.support.google.com/google-ads/answer/1704368?hl=en>. See also ICO, *Democracy Disrupted, supra* note 3 at 41-42 (noting that for all the online platforms the "full range of advertising services are available to political parties and campaigns in the same way as they are to all other organizations"); McEvoy, *Full Disclosure*, *supra* note 5, at 25; OPC and OIPC BC, *Joint Investigation of AggregateIQ Data Services*, *supra* note 5.
56. As an example of non-users' data entering the data market, the Canadian company uCampaign's mobile app asks app users for permission to access their address books and employs "gamification" strategies to motivate people to engage with political campaigns by awarding users points for sending texts and emails to contacts. See Digital, Culture, Media and Sport Committee, *Disinformation and 'Fake News' Interim Report*, *supra* note 5 at paras 121-22. See also Aleksandra Korolova, "Privacy Violations Using Microtargeted Ads: A Case Study" (2011) 3 J Privacy & Confidentiality 27-49; David Ingram, "Facebook Fuels Broad Privacy Debate by Tracking Non-Users" *Reuters* (15 April 2018), online: <www.reuters.com/article/us-facebook-privacy-tracking/facebook-fuels-broad-privacy-debate-by-tracking-non-users-idUSKBN1HM0DR>; Rob Price, "Facebook Collects Data on Non-Users for 'Security' – Here's the Whole Story" *Business Insider* (11 April 2018), online: <www.businessinsider.com/mark-zuckerberg-facebook-collects-data-non-users-for-security-2018-4>.
57. Between 2010 and 2014, Facebook had "Friends Permissions," which "allowed developers to access data related to users' friends, without the knowledge or consent of those friends." After 2014, some of these practices continued. GSR, the company owned by the Cambridge professor whose research was used by Cambridge Analytica, relied on a "pre-existing application functioning under Facebook's old terms of service" after Facebook revised their terms of service to prevent that kind of data scraping. Digital, Culture, Media and Sport Committee, *Disinformation and 'Fake News' Interim Report*, *supra* note 5 at paras 102, 105; ICO, *Investigation into the Use of Data Analytics in Political Campaigns*, *supra* note 5 at 30-31.
58. See *e.g.* Gabriel JX Dance, Michael LaForgia & Nicholas Confessore, "As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants" *New York Times* (18 December 2018), online: <www.nytimes.com/2018/12/18/technology/facebook-privacy.html>.

Typically in campaigns' voter databases, voters are assigned scores that measure their political leaning, which is extrapolated from the amalgamated data.[59] This "persuadability score" influences whether an individual is contacted by a candidate, by what communication method, and how much effort is put into convincing them to vote or delivering them to the polls. As these scoring schemes have matured, they encompass ever-more personal information from more sources. The score is used to allow campaigns to effectively target voters, thereby producing more efficient campaign tools, such as walk lists, phone lists, email lists, and lawn sign allocations.[60] Persuadability scores can be especially effective for mobilizing marginal voters who are instrumental in close elections, enabling parties to target swing voters or the geographical areas where ridings are in play.

Left unchecked, the future of data-driven campaigns will become even more individualised and data-dependent, and accordingly pose more serious challenges for voter privacy. A 2018 study for the UK Information Commissioner identified seven trends for data analytics in political campaigns: detailed audience segmentation to create more granular categories and more atomization of voters; cross-device targeting through geolocation data and the Internet of Things to identify data across multiple devices as belonging to a single person and to customise messages for a "segment of one"; growth in psychographic techniques and facial recognition to target messages by emotional state; use of artificial intelligence to measure and improve campaign messages in real time; use of artificial intelligence to automatically generate bespoke advertising based on an individual's interactions with chatbots; use of mass personal data to improve the prediction of election results; and new delivery platforms for campaign messages such as wearables, smart TV, and virtual reality.[61] Not all of these practices are evident yet in Canada. Any new technology that gathers relevant information about voters, however, will eventually be useful to political parties. The import of these trends is a coalescence toward customising unique messages for an audience of one voter. Accordingly, campaigns "will be incentivised to hold or obtain more personal data on individuals, and to collect as much diverse data as possible, in order to maximise the effectiveness of their messaging."[62]

---

59. Belfry Munroe & Munroe, *supra* note 12 at 12. For example, in CIMS each voter in the database is assigned a score of -15 to +15, while the Liberalist scoring ranks voters on a scale of 1 to 10.
60. Delacourt, *supra* note 37 at 246-47, 254-55.
61. Bartlett, Smith & Acton, *supra* note 3 at 27-37.
62. Bartlett, Smith & Acton, *supra* note 3 at 38.

The particular ways in which political campaigners use data analytics have important implications for the quality and extent of engagement between parties and Canadians, with a resulting impact on voter privacy and democracy.[63] First, microtargeting enables politicians to home in on the segment of the population that is likely to vote for them and, by extension, enables parties to identify voters who are very *unlikely* to vote for them. Rather than designing messages for the entire population or a region, the rational calculus for parties with scarce resources is to mobilise the voters most likely to support them and not to waste precious time and money attempting to contact or persuade individuals who are likely to be unreceptive. For instance, the Liberal Party database has "the capacity to sort neighbourhoods for canvassing, to identify which houses were worth visiting and which houses were not."[64] A candidate seeking to cover as much ground as possible during canvassing could use metrics to determine that it was only worth knocking on the doors of some houses on a street. The Council of Europe has warned of such "political redlining," meaning the deliberate lack of engagement by a party with voters who have been identified by the data as unlikely to vote or as being part of a constituency that is not necessary to win an election.[65] The Council has cautioned that the redlining effects can be compounded in subsequent elections as data from past elections influences future campaign choices.

More sinisterly than the risk that some voters will be ignored by some parties, microtargeting also raises the spectre of direct voter suppression. If big data analytics designed to predict the intentions of voters can be used to mobilise turnout, it can also be used to suppress it. Voter suppression tactics include any communication designed to dissuade an individual from casting a ballot, including circulating disinformation regarding voting procedures. The kind of misleading automated phone calls designed to suppress turnout in the "robocalls"

63. Solon Barocas identified four ways that microtargeting contributes to undermining democracy: (1) an increased willingness and ability to deliver messages on wedge issues that would be extremely divisive in a more public forum; (2) voter discrimination and de facto disenfranchisement; (3) a chilling of political participation due to perceived violations of voters' privacy; and (4) a general trend toward single issue politics that leads to increased partisanship among voters and ambiguous political mandates for elected representatives. Solon Barocas, "The Price of Precision: Voter Microtargeting and Its Potential Harms to the Democratic Process" (PLEAD '12: Proceedings of the First Edition Workshop on Politics, Election, and Data, ACM New York, November 2012), (2012) ACM 31.
64. Delacourt, *supra* note 37 at 287.
65. Council of Europe, Committee of Experts on Media Pluralism and Transparency of Media Ownership, *Feasibility Study on the Use of Internet in Elections*, MSI-MED 3rd Meeting (2017) at 13 [COE, *Feasibility Study on the Use of Internet in Elections*].

scandal during the 2011 Canadian federal election could be replicated through online communications with the same intent.[66] The "robocalls" gave misleading information about where individuals could vote and some involved fraudulent impersonation of Elections Canada officials. Attempts by foreign actors at voter suppression in the 2016 United States presidential election involved interference through social media platforms and relied on data analytics to carry them out.[67]

Second, the manner in which parties use big data analytics encourages the treatment of voters as consumers. The precision of modern microtargeting by political parties depends on combining information traditionally considered to have political relevance with insights drawn from other information, such as consumer purchases. Modern campaign practices of Canadian political parties conflate the individual as consumer and the individual as citizen, thereby producing campaign strategies that closely emulate marketing strategies designed for consumers.[68]

Third, microtargeting may provide incentives for negative messaging and wedge issues, which could result in more divisive campaigns.[69] The United Kingdom's report on disinformation characterised it as "relentless targeting of hyper-partisan views, which play to the fears and the prejudices of people, in order to alter their voting plans."[70] As a research consultancy cautioned, "there is a danger that political messaging will become more emotional in tone, appealing more often to anger, frustration or prejudice, in an attempt to mobilise voters and maximise engagement with content," which is "likely to have other, longer term effects on the health of democracy."[71] Microtargeting could exacerbate the effects of echo chambers (content from like-minded individuals) and filter

66. See Michael Pal, "Canadian Election Administration on Trial: 'Robocalls,' *Opitz*, and Disputed Elections in the Courts" (2017) 28 King's LJ 324.
67. See US, Robert S Mueller, *Report on the Investigation Into Russian Interference in the 2016 Presidential Election*, vol 1 (Department of Justice, March 2019). See especially *ibid* at 24-26.
68. Delacourt, *supra* note 37.
69. COE, *Feasibility Study on the Use of Internet in Elections*, *supra* note 65 at 12-13.
70. Digital, Culture, Media and Sport Committee, *Disinformation and 'Fake News' Interim Report*, *supra* note 5 at para 92.
71. Bartlett, Smith & Acton, *supra* note 3 at 40.

bubbles (algorithmically-selected content based on presumptions of the user's interests), which magnify confirmation biases.[72]

Fourth, big data campaign practices based on *incorrect* information about voters or faulty techniques of analysis can limit interactions between candidates and voters. If a party relies on data analysis based on faulty inferences that draw incorrect conclusions about a voter's persuadability, the party could fail to contact a voter who actually could have been swayed. If a candidate sends direct mail advertising with strong messaging to an eligible voter who is slightly undecided but is leaning towards the opposing candidate, then the advertising could inadvertently provoke the voter to vote for the opposing candidate.[73] Not only are individuals with an incorrect persuadability score less likely to hear the platforms that they would have been receptive to, they may also be systematically excluded from the process of shaping the party's platforms.

Fifth, parties' use of detailed voter profiles has privacy implications for individuals regardless of whether the data profiles lead to accurate inferences. Whether or not big data collection and analysis is accurate enough to help the campaigns, there are significant privacy implications of campaigns collecting, storing, and analyzing vast amounts of personal information about voters and making important decisions about voters' "persuadability" based on that analysis. The logic of big data is that there is never enough: More data supposedly produces more accurate inferences. The incentives in data-driven campaigns will continue to push for parties to collect ever more personal information about voters continuously and ubiquitously in an effort to generate more accurate predictions than the other campaigns.

At this stage, it is unclear whether big data analytics is producing the desired effects for parties of better identifying likely voters and better honing messages to persuade those people to vote. There are some indications that the advantages

---

72. See Cass R Sunstein, *Republic.com* (Princeton University Press, 2001) (on echo chambers); Eli Pariser, *The Filter Bubble: How the New Personalized Web is Changing What We Read and How We Think* (Penguin, 2012) (filter bubbles); Damian Tambini et al, "The New Political Campaigning" (2017), online (pdf): *London School of Economics and Political Science* <eprints.lse.ac.uk/71945/7/LSE%20MPP%20Policy%20Brief%2019%20-%20The%20new%20political%20campaigning_final.pdf> (on filter bubbles and campaigns); Natali Hehlberger, "Exposure Plurality as a Policy Goal" (2012) 4 J Media L 65.
73. See SC Gwynne, "Retail Politics" (January 2006), online: *Texas Monthly* <www.texasmonthly.com/articles/retail-politics> at 1.

to the parties of extensive data profiles may be exaggerated.[74] One study found a single Facebook like by a voter for a politician in a multi-party system predicts voter intention as accurately as hundreds of heterogeneous likes.[75] Weighing the potential benefits and harms of big data campaigning for the quality and extent of individuals' interactions with political parties and for voter privacy is a complicated exercise. The personal information collected, stored, analyzed, and used by political parties fuels a host of strategies whose aggregate impact on democratic politics is not clear at this stage in the evolution of the technologies. If it is working as its proponents claim and the parties deploying these techniques hope, big data analytics facilitates political engagement and voter persuasion: It helps parties to be responsive to voters' concerns and to communicate to voters in the manner most conducive to voters understanding parties' policies and being persuaded to vote for them. Even the rosiest picture of the use of big data in federal politics, however, must acknowledge that it has transformed campaigning and the practices of political parties in significant ways that should be addressed, including safeguarding voter privacy. An optimistic view of the benefits of big data in politics does not justify the hands-off attitude of current electoral and privacy law toward political parties with regard to voter privacy. We turn in the next section to explaining why the existing legal framework is flawed and does not adequately protect voter privacy.

74. See *e.g.* Colin Bennett, "How Campaign 'Micro-Targeting' Works—And Why It Probably Doesn't" (9 September 2015), online: *iPolitics* <ipolitics.ca/2015/09/09/how-campaign-micro-targeting-works-and-why-it-probably-doesnt/> (on the inability to determine whether political campaigns are successful because of their reliance on big data or in spite of it).

75. Jakob Bæk Kristensen et al, "Parsimonious Data: How a Single Facebook Like Predicts Voting Behavior in Multiparty Systems" (2017) 12 *PLoS ONE* e0184562, online: <doi.org/10.1371/journal.pone.0184562> (finding that "a few, but selective digital traces produce prediction accuracies that are on par or even greater than most current approaches based upon bigger and broader datasets"). See also Joshua L Kella & David E Broockman, "The Minimal Persuasive Effects of Campaign Contact in General Elections: Evidence from 49 Field Experiments" (2018) 112 *Am Pol Sci Rev* 148 at 148 (finding that, based on a meta-analysis of 49 field experiments, "the best estimate of the effects of campaign contact and advertising on Americans' candidate choices in general elections is zero").

II. THE EXISTING LEGAL FRAMEWORK FOR VOTER PRIVACY

A. THE *PRIVACY ACT* AND *PIPEDA*

Privacy concerns with voter data arise not only because of the centrality of personal information to the activities of political parties and the availability of ever-more sophisticated technologies with which to analyse it, but also because those activities are largely unregulated by privacy legislation or by elections law.[76] Although the *CEA* confers some protections to voters' personal information,[77] it does not specifically regulate voter privacy nor significantly restrict the use of personal information by political parties if used for purposes related to elections.[78] Further, even though electors may opt out of the Register,[79] political parties can continue to collect information about voters who have exercised their opt-out.

Political parties are not currently subject to federal privacy legislation regarding the collection, storage, and use of personal information. The two main pieces of privacy legislation federally are the *Privacy Act* and *PIPEDA*. Political parties are clearly not covered by the *Privacy Act*, which applies to the public sector. Canada's *Privacy Act* was designed with the intent to "protect the privacy of individuals with respect to personal information about themselves held by a government institution" and to "provide individuals with a right of access to that information."[80] The *Privacy Act* applies only to "government institutions."[81] "Government institution" is defined under section 3 of the *Privacy Act* as "any department or ministry of state of the Government of Canada, or any body or office, listed in the schedule, and…any parent Crown corporation, and any wholly-owned subsidiary of such a corporation…."[82] Political parties are heavily

76. See Fenwick McKelvey & Jill Piebiak, "Does the Difference Compute? Data-Driven Campaigning in Canada," in Mireille Lalancette, Vincent Raynauld, & Erin Crandall, eds, *What's Trending in Canadian Politics? Understanding Transformations in Power, Media, and the Public Sphere* (UBC Press, 2019) at 208; Bennett & Bayley, *Canadian Federal Political Parties and Personal Privacy Protection*, *supra* note 32.
77. As noted above, s 2(1) of the *CEA* adopts the same definition for "personal information" as that used in s 3 of Canada's *Privacy Act*. See *CEA*, *supra* note 8, s 2(1); *Privacy Act*, *supra* note 6, s 3.
78. *CEA*, *supra* note 8, s 111(f). The provision states that "no person shall… (f) knowingly use personal information that is recorded in a list for a purpose other than (i) to enable registered parties, eligible parties, members or candidates to communicate with electors in accordance with section 110, or (ii) a federal election or referendum."
79. Elections Canada, "Description of the National Register of Electors," *supra* note 21.
80. *Privacy Act, supra* note 6, s 2.
81. *Ibid*, s 3.
82. *Ibid*.

regulated by electoral regulation but are independent, private entities. They are not departments or ministries or Crown corporations for purposes of section 3 and are not mentioned in the Schedule. Political parties therefore operate outside of the *Privacy Act.*

PIPEDA is the federal privacy legislation pertaining to the private sector. Although political parties are not *explicitly* exempt from the statute, they are outside its jurisdiction when engaged in traditional political activities. *PIPEDA* applies to all provinces except the three provinces that have "substantially similar" private-sector data protection legislation.[83] *PIPEDA* incorporates the set of ten fair information principles that are commonly used internationally in legislation and regulatory instruments as a framework to protect personal information.[84] Personal information is defined in *PIPEDA* as "information about an identifiable individual,"[85] which is a broad enough phrase that it would otherwise capture information about voters gathered by parties. *PIPEDA* applies, however, only to an organization that "collects, uses, or discloses [personal information] in the course of *commercial activities.*"[86] "Commercial activities" are defined as "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists."[87] Political parties must have a "political purpose" in order to be registered under the *Canada Elections Act*.[88] Parties generally do not engage in "commercial activities" within the meaning of *PIPEDA* when they are engaged in activities that have a "political" purpose.[89] Political parties, accordingly, would generally be unregulated by *PIPEDA* in how they collect, store, and use data about voters. This would be true even if the

83. See Alberta, *Personal Information Protection Act*, SA 2003, c P-6.5; British Columbia, *Personal Information Protection Act*, SBC 2003, c 63 [*BC PIPA*]; Québec, *An Act Respecting the Protection of Personal Information in the Private Sector*, RSQ c P-39.1.
84. The ten fair information principles are: (1) Accountability; (2) Identifying Purposes; (3) Consent; (4) Limiting Collection; (5) Limiting, Use, Disclosure, and Retention; (6) Accuracy; (7) Safeguards; (8) Openness; (9) Individual Access; and (10) Challenging Compliance. See *PIPEDA*, *supra* note 7, Schedule I.
85. *PIPEDA*, *supra* note 7, s 2(1). Personal information also includes inferences about an identifiable individual. See *e.g.* ICO, *Democracy Disrupted*, *supra* note 3 at 30.
86. *PIPEDA*, *supra* note 7, s 4(1) (emphasis added).
87. *Ibid*, s 2(1).
88. *CEA, supra* note 8, s 2(1).
89. Bennett & Bayley, *Canadian Federal Political Parties and Personal Privacy Protection*, *supra* note 32.

parties obtain voter data from a commercial organization such as a databroker that is itself subject to *PIPEDA*.[90]

B. OTHER LEGISLATION ON VOTER PRIVACY

There are other pieces of potentially relevant legislation that provide rights related to the control of personal information or that protect voter privacy in limited contexts. First, provincial privacy law applies in British Columbia to riding associations of both provincial and federal political parties in the province. In British Columbia, the *Personal Information and Protection Act* (*PIPA*) defines the "organizations" to which it applies more broadly than the definition of "organization" under *PIPEDA*.[91] While it has been clear that the BC provincial privacy statute's broader definition applied to *provincial* political parties, the BC Information and Privacy Commissioner has ruled that it also applies to the electoral district associations in the province of federal parties registered under the *CEA*.[92]

There are also federal statutes beyond *PIPEDA* and the *CEA* that may be relevant to voter information in some situations. The *Access to Information Act*[93] permits individuals to request information on specific topics from a "government institution,"[94] and thus might seem to provide an avenue for individuals to access the information that parties hold about them. Political parties are not subject to the access to information regime, however, by virtue of their exclusion from the list of "government institutions" subject to the *Access to Information Act*.[95]

The *Telecommunications Act* and associated rules and regulations apply to some aspects of communications between political entities and voters, including

---

90. It is possible that a political party could be engaging in a "commercial activity" for purposes of *PIPEDA,* if, for example, it were to sell membership lists for non-political purposes. See *PIPEDA*, *supra* note 7, s 2(1).
91. *BC PIPA*, *supra* note 83, s 3(1) (defining organization to include a person, an unincorporated association, a trade union, a trust, and a non-profit organization); *ibid*, s 3(2) (exceptions, which do not apply to political parties); *PIPEDA*, *supra* note 7, s 2(1) (defining organization to include an association, partnership, a person, and a trade union).
92. *Re Courtenay-Alberni Riding Association of the New Democratic Party of Canada* (28 August 2019), 2019 BCIPC 34, Order P19-02 online (pdf): <oipc.bc.ca/orders/2331> [Order P19-02]. The ruling held that because the pith and substance of *PIPA* was to regulate data protection and not to regulate elections, it was not unconstitutional for the provincial privacy statute to apply to federal parties. *Ibid* at paras 1, 95.
93. RSC 1985, c A-1.
94. *Ibid*, s 2(1).
95. *Ibid*, Schedule I.

email, phone, and text contacts.[96] Political parties and candidates are exempt from the National Do Not Call List that pertains to unsolicited telemarketing calls, but they must maintain an internal do-not-call list.[97] The principled reason for their exemption is that parties need to be able to communicate directly with voters (including by telephone), and therefore, if individuals were allowed to block contact from parties, it would undermine a relationship that is necessary in a democracy. A less charitable reading would be that the Parliamentarians who voted on the law may have had their own interests in mind in exempting candidates, parties, and other political entities.

Political parties are also largely excluded from national anti-spam legislation, which limits unsolicited email communications, if parties are soliciting opinions or contributions.[98] However, there are regulations to increase transparency around communications with voters during elections.[99] The Canadian Radio-Television and Communications Commission (CRTC) and Elections Canada have signed a joint memorandum of understanding on how to jointly regulate "Voter Contact Calling Services" during elections.[100] Both the CRTC and Elections Canada have legislative roles, under the *Telecommunications Act* and the *CEA* respectively, to regulate communications with electors. These rules and agency practices have restricted some forms of voter contact.[101] The CRTC oversees a "Voter Contact Registry" to protect Canadians from misleading phone calls during elections and increase accountability.[102] Political parties and candidates are also prohibited

---

96. SC 1993, c 38, s 41.7. See CRTC, "Rules for Unsolicited Telecommunications Made on Behalf of Political Entities" (17 March 2019), online: *CRTC* <crtc.gc.ca/eng/phone/telemarketing/politi.htm> (for a summary of the *Telecommunications Act*).
97. The Do Not Call List has exceptions permitting unsolicited telemarketing calls from political parties, candidates, and riding associations, as well as registered Canadian charities, pollsters, and newspapers. See CRTC, "Unsolicited Telecommunications Rules" (31 March 2013) at Part II, online: *CRTC* <crtc.gc.ca/eng/trules-reglest.htm>.
98. *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, SC 2010, c 23 at s 13 ["Anti-Spam Legislation"].
99. For an overview of the applicable rules, see CRTC, "Rules for Unsolicited Telecommunications Made on Behalf of Political Entities," *supra* note 97.
100. Memorandum from CRTC & Elections Canada, "Memorandum of Understanding" (1 April 2015), online: *Elections Canada* <elections.ca/content.aspx?section=abo&dir=mou/crtc&document=index&lang=e>.
101. *Telecommunications Act*, *supra* note 96, ss 41-41.7, 72.01-72.15; *CEA*, *supra* note 8, ss 348.02, 348.03, 348.04.
102. *CEA*, *supra* note 8, ss 348.02, 348.03, 348.04.

from using pre-recorded "robocalls" to contact voters for solicitations unless there is explicit consent.[103]

This balanced approach of allowing political parties to contact voters who have not opted out, but regulating the contact to reduce fraudulent and misleading communications, is sound for an electoral democracy where informed individual participation is important. Without the connection between voters and those that seek to represent them, electoral democracy cannot function properly. Democracy requires individual participation and that parties be able to interact with those whom their candidates seek to represent. Parties need to know the concerns of the electorate in order to represent them in a democracy. At the same time, voter privacy is an important consideration. With reference to the Voter Contact Registry, the CRTC explains that "the desire to connect with voters must be tempered with respect for Canadians' privacy and the protection of their right to refuse to be contacted by individuals or political groups if they so choose."[104] These CRTC rules address voter privacy in the specific context of unsolicited telecommunications to voters on behalf of political entities. But they were not designed to have, and have not had, a meaningful impact on voter privacy in general and do not attempt to address big data analytics.

C. SELF-REGULATION BY POLITICAL PARTIES

Before 2018, in the absence of any clear legislative requirements on voter privacy, political parties regulated themselves through their own privacy policies.[105] All of the major federal parties, the Liberal Party of Canada, Conservative Party of Canada, New Democratic Party, Bloc Québécois, and Green Party of Canada,

103. CRTC, "Unsolicited Telecommunications Rules," *supra* note 97 at Part IV.
104. CRTC, "Protecting You from Rogue and Misleading Calls During Elections" (25 July 2019), online: *CRTC* <crtc.gc.ca/eng/phone/rce-vcr/guidecan.htm#infograph-can>.
105. See Dara Lithwick, "Privacy and Politics: Federal Political Parties' Adherence to Recognized Fair Information Principles" (2016) 10 JPPL 39; Colin J Bennett, "Data-Driven Elections and Political Parties in Canada: Privacy Implications, Privacy Policies and Privacy Obligations" (2018) 16 CJLT 195 [Bennett, "Data-Driven Elections"].

have privacy policies available on their websites.[106] These policies, however, do not explicitly reference the use of the parties' respective voter management systems and offer relatively little detail on the type of data that is stored in their databases and the manner in which it is used. It is difficult, because of the policies' vague wording, for voters to know whether their provisions pertain solely to the political parties' websites or apply to a fuller range of their activities, including the databases.[107] The parties' privacy policies accord individuals some rights consistent with fair information principles, modified to account for federal elections requirements such as recordkeeping pertaining to campaign financing. The parties' level of compliance with their own internal policies has been unclear, however, because prior to the *CEA* amendments in 2018 the parties did not have privacy reporting obligations and post-2018 there are only minimal ones.[108]

The parties' privacy policies include some statements about the downstream uses of personal information, such as whether voter data may be shared with, or sold to, data intermediaries, or whether voter information can be shared with local ridings. The policies have not been explicit about data procurement, such as whether personal information is obtained from third-party aggregators.[109] It has also been unclear whether voter data is surrendered to outside entities.[110] Nor has it been clear what data security measures (*e.g.*, encryption and prohibiting data transfer to USB keys) political parties are currently using to protect voters' personal information against hacking and other data leaks.[111] The Communications Security Establishment, Canada's outward facing national security agency, concluded in recent reports that a lack of security protections

106. See Liberal Party of Canada, "Privacy Policy" (last visited 25 October 2020), online: *Liberal Party of Canada* <liberal.ca/privacy>; Conservative Party of Canada, "Privacy Policy" (last visited 25 October 2020), online: *Conservative Party of Canada* <conservative.ca/privacy-policy>; Green Party of Canada, "Important Information and Privacy Policy" (last visited 25 October 2020), online: *Green Party of Canada* <greenparty.ca/en/privacy>; BLOC Québécois, "Politique de protection des renseignements personnels" (last visited 25 October 2020), online: *BLOC Québécois* <www2.blocquebecois.org/politique-de-protection-des-renseignements-personnels>; New Democratic Party of Canada, "Privacy Policy" (last visited 25 October 2020), online: *New Democratic Party of Canada* <ndp.ca/privacy>.
107. See Colin Bennett, "So You Just Want Politicians to Leave You Alone? Good Luck With That" (24 August 2015), online: *iPolitics* <ipolitics.ca/2015/08/24/so-you-just-want-politicians-to-leave-you-alone-good-luck-with-that>; Bennett, "Data-Driven Elections," *supra* note 105; Judge & Pal, "Privacy and the Electorate," *supra* note 49.
108. *CEA, supra* note 8, s 385(2)(k), s 385(4), s 385.1
109. Bennett, "Data-Driven Elections," *supra* note 105.
110. Howard & Kreiss, *supra* note 42 at 28.
111. See Bennett & Bayley, *Canadian Federal Political Parties and Personal Privacy Protection*, *supra* note 32 at 22-24 (for an account of some notable voter privacy breaches in Canada).

for the data that political parties hold about voters contributes to parties being targeted by hostile foreign entities for digital interference.[112]

Under self-regulation, the existing political parties' privacy policies have varied with regard to consent.[113] The parties' practices, unclear privacy policies, and vulnerabilities with respect to parties' data acquisition, data sales, and data security have significant implications for voter privacy and undermine voters' ability to meaningfully decide whether to consent to their data being collected and used. It is difficult for individuals to understand what data parties hold about them and what they are doing with it. The policies are unclear about which activities are covered under the policies and particularly unhelpful about key aspects of big data practices, such as the type of data that is collected and the sources from which it is obtained. A party could have multiple privacy policies, produced for different purposes, not all of which are comprehensive or made publicly available online. Although each policy may be requested by the public, it is difficult for someone to know that policies other than those online even exist so as to be able to make such a request.[114]

There is also a lack of transparency around political parties' use of databrokers, the degree to which campaigns rely on them, and whether the resulting profiles are accurate predictors of voter behaviour. In addition, it is difficult to determine with exactitude the types of inferences that are being made, the precise volume of data on each prospective voter, the precision of their micro-targeting techniques, the efficacy of such techniques, the types of messages delivered to voters, the use of such tactics outside the election period, and the extent to which some people are at risk of being excluded from political messages simply by virtue of their persuadability score.

Self-regulation of voter privacy by political parties has been wholly insufficient for voter privacy protection. Political parties are heavily regulated entities in nearly all other aspects. They are exempt from current privacy law because MPs, who are overwhelmingly affiliated with a political party, have not made political parties subject to the privacy rules that apply to the public and private sectors. With

---

112. Communications Security Establishment, *Cyber Threats to Canada's Democratic Process* (Communications Security Establishment, 2017) [CSE, *Cyber Threats*]; Communications Security Establishment, *2019 Update: Cyber Threats to Canada's Democratic Process* (Communications Security Establishment, 2019) [CSE, *2019 Update*]. See also David Thaw, "From Russia with Love" (2019) University of Pittsburgh Legal Studies Research Paper No 2019-32, online: <*ssrn.com/abstract=3038308*>.
113. See Judge & Pal, SSHRC Knowledge Synthesis Grant, *supra* note 49; Bennett, "Data-Driven Elections," *supra* note 105.
114. McEvoy, *Full Disclosure*, *supra* note 5 at 35.

the widespread use of big data analytics among federal political parties, the legal status quo is unsustainable. The potential for the misuse of personal information about individual voters is enormous. There is no enforcement mechanism for violations of a party's privacy policy and, indeed, a voter is unlikely to even hear about any misuse as there is no reporting obligation either. The regulation of databrokers and intermediaries, as commercial entities subject to *PIPEDA*, may provide some protection for voter information, but it does not protect voters once the data is in the hands of parties, which can acquire, analyze, and share the data without regulatory restraint if they do so for a political purpose.

Parliament sought to address some of these deficiencies in 2018 with the voter privacy provisions of the *EMA.* Though an important first step, we argue in the next section that these amendments in the *EMA* were inadequate to protect voter privacy.

D. THE START OF MEANINGFUL REGULATION? THE *ELECTIONS MODERNIZATION ACT*

The 2018 *EMA* is the first time that Parliament has obliged parties to address the voter privacy issue and hence moves, to a modest degree, away from the largely self-regulatory model that previously prevailed. The *EMA* mandates that political parties adopt a "policy for the protection of personal information."[115] Existing parties must file privacy policies with Elections Canada, provide a public internet link to the policy, name an officer responsible for administering the policy, and ensure updates are transmitted to Elections Canada. According to the *CEA*, parties must specify the types of information they collect and how they do so, how they protect and use that information, whether the information is sold, how they train those who have access to the information, and their practices regarding the collection of information online and use of cookies.[116] The penalties for breaching the obligations in the *EMA* are significant, with parties that fail to comply facing potential deregistration.[117] Deregistration means that a party would no longer have the benefits of party status under the *CEA* and could not contest federal elections as a single entity. New parties will have their applications for registered party status rejected if they do not comply with the privacy policy requirements in the *EMA*.[118]

---

115. *CEA*, *supra* note 8, s 385(2), as amended by *EMA*, *supra* note 13, s 254(1).
116. *CEA*, *supra* note 8, ss 385(2)(k), 385(4), 385.1.
117. *Ibid*, s 385.1(2).
118. *Ibid*.

While an important first step, the measures in the *EMA* are still inadequate to protect the personal information of voters. First, although the *EMA* requires that each registered party have a privacy policy, the requirement is nominal. The legislation simply outlines that the parties must have a privacy policy describing their approach to data collection, retention, and use, but it does not impose substantive privacy criteria for these policies. It does not require that they adhere to the fair information practices set out in *PIPEDA* or the *Privacy Act*, nor does it establish other privacy standards tailored to political parties. As the BC Information and Privacy Commissioner described of the limited import of section 385 of the *CEA*, "it imposes no substantive requirements relating to the collection, use or disclosure of personal information," and is "in substance merely a transparency measure."[119] Hence the *EMA* codifies the existing, flawed practice under self-regulation whereby parties have privacy policies, but where the policies have little impact on the actual protection of voter privacy.[120]

Second, there is no enforcement mechanism to examine the accuracy and sufficiency of statements made by the parties. Deregistration is a blunt instrument that is rarely used by the CEO, and it is difficult to imagine a CEO deregistering one of the major parties for failing to update its privacy policy. New parties can easily meet the standard by simply having a policy that states what they choose to do. There is no authority for the CEO to sanction a party for breaching its own rules or for adopting rules that fall below some minimum standard since threshold standards are not specified by the amendments. In jointly prepared guidance in 2019 for political parties to comply with the new *EMA* requirements, the Office of the Privacy Commissioner (OPC) and CEO remarked that "the new law prescribes some elements of content [but] it does not require that content comply with international privacy standards."[121] Their guidance accordingly consisted of one page on the legally proscribed content and several pages on hortatory recommendations. Open Media, in a 2019 report, examined whether federal parties' policies complied with the joint guidance on recommended practices and

119. Order P19-02, *supra* note 92, at para 70.
120. See Bennett, "Data-Driven Elections," *supra* note 105.
121. Office of the Privacy Commissioner of Canada, "Guidance for Federal Political Parties on Protecting Personal Information" (1 April 2019), online: <www.priv.gc.ca/en/privacy-topics/collecting-personal-information/gd_pp_201904> [OPC, "Guidance for Federal Political Parties"].

found, at best, that the parties attained partial credit in some areas and, in most cases, they had failing grades.[122]

Third, the *EMA* is revealing with regard to some existing political party practices. Section 385(2)(k)(iii) of the *CEA* (as amended by the *EMA*) requires parties to set out in their official policies "under what circumstances that personal information [collected by the party] may be sold to any person or entity."[123] The legislation thus acknowledges, but does not prohibit, the practice of parties commercializing voter data; this has further problematic implications as it suggests that the sale of voter data by political parties is also not covered as a "commercial activity" under *PIPEDA*.

The *EMA* is therefore no more than a first step. It expands the regulatory ambitions of the *CEA* to include voter privacy and the protection of personal information, which is an important move forward. Without further reforms, however, the *EMA* will be incomplete and potentially harmful if it provides the illusion of movement toward voter privacy and decreases the urgency around the issue.

III. REFORMING VOTER PRIVACY: BEYOND THE *EMA*

Canadian law needs to be updated to reflect the serious repercussions for voter privacy of digital campaigning and data-driven elections. The current legal framework under both elections law and privacy law is inadequate for voter privacy. The status quo of self-regulation by political parties, augmented by the requirement from the *EMA* that all parties have a privacy policy, does not provide adequate privacy protection through elections law. The amendments in the *EMA* were minor and, more formal than substantive, did not provide significant privacy protection to voters. Privacy law, meanwhile, has left political parties out of both the public and private sector legislation. In this Part, we detail how voters' privacy should be protected and how political parties should be regulated.

There are several plausible legislative options for regulating political parties to protect voter privacy. The first option would be to include political parties under one of the existing federal privacy statutes. The second main legislative option would be to amend the *CEA* again to impose privacy obligations on

122. Open Media, "Canada's Political Parties Privacy Policies: An Assessment Against Best Practices Defined by Elections Canada and the Office of the Privacy Commissioner" (2019), online: <openmedia.org/article/item/how-do-they-score-we-rated-new-privacy-policies-all-major-parties-and-every-single-one-failed-key>.

123. *EMA*, *supra* note 13, s 254(1).

parties that are stricter than those added in 2018 by the relatively anemic privacy provisions in the *EMA*.[124]

A. EXISTING PRIVACY LEGISLATION: THE *PRIVACY ACT* AND *PIPEDA*

Placing political parties under the auspices of either of the existing privacy statutes would be counter-productive. The *Privacy Act* is not a realistic model given that political parties, although heavily regulated, are still private entities and very different from the government departments and Crown corporations subject to that law. If political parties were to be incorporated under the ambit of one of the existing federal privacy statutes, the critical consensus has leaned heavily toward *PIPEDA* as the better option.[125]

The problem with the *PIPEDA* approach, however, is that *PIPEDA* has been widely criticized for being out of date, inadequately addressing new technologies, lacking strong investigatory and enforcement mechanisms, and not implementing higher standards for privacy protection in the private sector.[126] There have frequently been calls from Parliament and the academic community to revise *PIPEDA*.[127] The Trudeau government's proposed "Digital Charter" of May 2019 signalled its intent to significantly amend *PIPEDA*.[128] Due to a lack of details in the Digital Charter, it remains to be seen precisely how it would do so and the extent of the changes. It is also not clear whether those changes will be implemented, given that the Liberal government was reduced to a minority in the October 2019 federal election.

Merely incorporating political parties in *PIPEDA*'s existing framework without also making significant changes to *PIPEDA* would not provide adequate privacy for voters. As *PIPEDA* has not been updated for algorithmic processing, even if political parties were to be added to the jurisdiction of *PIPEDA* it would not prevent political parties from engaging in big data practices; rather,

---

124. A third possibility would be stand-alone legislation with a privacy framework specifically designed for parties, but this approach seems unlikely, in our view, given the existence of federal electoral and privacy legislation. We do not consider this option in detail here. In any event, our recommendations on the content and jurisdiction would be the same.
125. See Bennett, "Data-Driven Elections," *supra* note 105; Lithwick, *supra* note 105; ETHI, *Towards Privacy by Design*, *supra* note 5.
126. See ETHI, *Towards Privacy by Design*, *supra* note 5 at 5-6, 20-32, 60-69; OPC, *Trust but Verify*, *supra* note 5.
127. See ETHI, *Towards Privacy by Design*, *supra* note 5 at 8-11 (on attempts at legislative amendment), 16-18 (on academic criticism regarding consent).
128. Innovation, Science and Economic Development Canada, *Strengthening Privacy for the Digital Age: Proposals to Modernize the Personal Information Protection and Electronics Documents Act*, (2019), online: <www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html> [ISEDC].

it would oblige the parties to adhere to fair information principles, including notice and consent.[129] But fair information principles, which already govern the private sector, have not protected Canadians against the mass data collection and analysis of their personal information. The problem is *not* that political parties have been left out of an effective privacy statute; if true, that could be remediated by amending *PIPEDA* to incorporate political parties. Rather, the problem is more far reaching as the existing privacy legislation has not worked well. Among other issues, *PIPEDA* suffers from a weak notion of consent that has failed to stem vast collection of data about individuals, weak enforcement mechanisms that has left the OPC with few serious compliance measures, and a legislative framework that has not been adequately updated to account for the seismic shifts wrought by big data.[130]

B. *THE CANADA ELECTIONS ACT*

The second option is to place the reforms in the main electoral legislation, the *CEA*. One of the main virtues of doing so is that Elections Canada is the agency with specialised and deep expertise in election administration. The *CEA* already regulates parties extensively and assigns responsibility for administering those provisions to the CEO. Parties are private entities, but with an important public role as an intermediary institution between voters and government. Elections Canada is in regular close contact with federal political parties as mandated by statute,[131] including through the provision of guidelines and interpretation notes, which are answers to questions posed by the parties about the agency's interpretation of various legal or administrative matters,[132] and the Advisory Committee of Political Parties,[133] where representatives of the parties provide

129. See *PIPEDA*, *supra* note 7.
130. See ISEDC, *supra* note 128; Office of the Privacy Commissioner of Canada, *Real Fears, Real Solutions: A plan for restoring confidence in Canada's privacy regime* (Annual Report to Parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act) Catalogue No IP51-1E-PDF (2017), online: <www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201617/ar_201617>; ETHI, *Towards Privacy by Design*, *supra* note 5; ETHI, *Towards Democracy Under Threat*, *supra* note 5; Standing Senate Committee on Transport and Communications, *Driving Change: Technology and the Future of the Automated Vehicle* (January 2018) (Chair: David Tkachuk), online (pdf): <sencanada.ca/content/sen/committee/421/TRCM/Reports/COM_RPT_TRCM_AutomatedVehicles_e.pdf>.
131. See *CEA*, *supra* note 8, s 21.1.
132. *Ibid*, s 16.1-16.5.
133. *Ibid*, s 21.1(1)-(4).

the CEO with "advice and recommendations."[134] Keeping electoral oversight under one roof is appealing as it would build on Elections Canada's existing expertise. One of the criticisms of the amendments that addressed the "robocalls" from the 2011 election was that it hived responsibility off to the CRTC, which is not as steeped in electoral matters as Elections Canada.[135] This approach potentially meant losing the benefit of Elections Canada's expertise in regulation of "robocalls." It also increased the burden on the regulated entities, namely the parties themselves, to interact with multiple regulators.

The *CEA* has steadily expanded its ambit over the last several decades to include regulation of entities and activities that were previously outside of its reach, including leadership campaigns and contestants, electoral district associations, social media platforms, and so on. The *EMA* took a first step to including privacy as well. Adding content to the framework established by the 2018 amendments in relation to privacy would not be at odds with the approach or scope of the *CEA* as a whole.

The drawback to this approach is that Elections Canada does not have specific expertise with privacy. The entity with expertise on privacy at the federal level is the OPC. While the CEO has expertise in dealing with political parties and understands the nuances of the political process, the OPC has expertise in data protection and understands the nuances of privacy-invasive activities. The OPC has jurisdiction over both the *Privacy Act* and *PIPEDA*. Giving the OPC jurisdiction over political parties in relation to voter privacy would be consistent with their mission to "protect and promote privacy rights" and may be most efficient from the perspective of individual voters. In either case, clear statutory language would be needed in order to render the grant of authority to oversee voter privacy to the particular agency. As Officers of Parliament, each is constrained by their specific home statutes.

In a 2013 report, the Chief Electoral Officer of Canada recommended that legislation be amended to grant Elections Canada jurisdiction over privacy breaches by political parties.[136] The report states:

> In order to preserve the confidence of Canadians in the political entities with whom they deal, and in order to better protect the privacy of Canadian electors dealing with political entities, it is recommended that the *Canada Elections Act* be amended

134. *Ibid*, s 21.1(2).
135. Michael Pal, "Electoral Management Bodies as a Fourth Branch of Government" (2016) 21 Rev Con Studies 85 at 93.
136. Chief Electoral Officer of Canada, *Preventing Deceptive Communication with Electors* (Ottawa: Elections Canada, 2013) [CEO, "Preventing Deceptive Communications"].

> to provide a mechanism by which the application of privacy protection principles governing most Canadian institutions and organizations would be extended to political parties.[137]

Responding to the report, the OPC agreed with the recommendation to impose privacy standards on political parties, but did not explicitly endorse the idea that Elections Canada be given the mandate:

> We welcome the report from Elections Canada, which highlights the fact that there is currently a gap in coverage under federal privacy legislation and suggests measures to address this gap. We feel this is an issue that warrants public discussion…We are pleased to see a recommendation that political parties should be required to meet these standards.[138]

Joint administration by both the federal privacy and election bodies is possible. Along the model of the *Copyright Act*, which is jointly administered by Canadian Heritage and Innovation, Science and Economic Development Canada (formerly Industry Canada), privacy obligations imposed on the political parties could be jointly administered by the CEO and the OPC.[139] This approach would have the advantage of specifically balancing democratic processes with voter privacy and could regulate political parties beyond defined campaign periods to acknowledge parties' continual interactions with the electorate.

If only one agency were to have jurisdiction over political parties' data practices, Elections Canada is the preferable option. Elections Canada is a non-partisan and independent agency with a mandate to administer and monitor compliance with the *CEA* and to conduct federal elections. It is likely to be better able to balance the special context of protecting personal information about voters along with the democratic need for political parties to be in communication with,

---

137. *Ibid* at 32.
138. Office of the Privacy Commissioner of Canada, News Release, "Statement from the Office of the Privacy Commissioner of Canada Regarding a Report by Elections Canada" (27 March 2013), online: <www.priv.gc.ca/en/opc-news/news-and-announcements/2013/nr-c_130327>.
139. ISEDC administers the *Copyright Act* through the Canadian Intellectual Property Office and develops copyright policy jointly with the Copyright Policy Branch of Canadian Heritage. See Canadian Intellectual Property Office, ISEDC, online: <www.ic.gc.ca/eic/site/cipointernet-internetopic.nsf/eng/Home>; Copyright Policy Branch, Canadian Heritage, online: <www.canada.ca/en/canadian-heritage/services/copyright-policy-branch.html>; Canada, Minister of Canadian Heritage and Minister of Industry, *Status Report on Copyright Reform* (24 March 2004), Submitted to the House of Commons Standing Committee on Canadian Heritage (2005), online: <www.ic.gc.ca/eic/site/crp-prda.nsf/eng/rp01133.html>.

and responsive to, voters. If this option is chosen, there should be amendments to the *CEA* that specifically grant Elections Canada this authority.

C. CONCLUSION ON LEGISLATION

Given the deficiencies in existing privacy legislation, we favour more stringent privacy protections specifically tailored to political parties and recommend that they be implemented through the *CEA* and with jurisdiction granted to the CEO. By separating oversight of voter privacy from the main agency on privacy writ large, the OPC, this approach would also foster an appreciation for how protection of voter privacy must be crafted with a view to the particular relationship between voters and parties and the role of parties in a democracy. The rest of this section details relevant considerations for crafting the content of stronger privacy protection specific to voters and parties.

D. GUIDELINES FOR VOTER PRIVACY REFORM

Such a framework should situate voter privacy as a limit upon the activities of political actors, but without stifling the connection between parties and voters that is essential to democratic life. To the extent possible, both the choices voters make about their own data and the ability of parties to be able to communicate with the electorate should be respected. The legislative model of data protection and its fair information principles are, at best, minimal requirements. Protecting voter privacy with data-driven campaigning requires a stronger privacy regime.[140] In the following guidelines, we acknowledge, but go beyond, fair information principles to build a privacy framework that is tailored to the specific context of voters and elections and that is cognizant of the particular impacts of big data analytics.

1. MANDATORY OBLIGATIONS

First, any privacy rules that apply to political parties must be mandatory. The *CEA* does not rely on voluntary regulation by parties of their other activities that are consequential to the electoral process and should not rely on self-regulation with regard to the protection of voters' personal information. The inadequacies of the current self-regulatory regime for parties have already been detailed in

140. For arguments that fair information principles are inadequate to deal with the privacy risks posed by big data, see Rubinstein, *supra* note 2 at 1; Woodrow Hartzog, "The Inadequate, Invaluable Fair Information Principles" (2017) 76 Md L Rev 952 at 954; Anna Romanou, "The Necessity of the Implementation of Privacy by Design in Sectors Where Data Protection Concerns Arise" (2018) 34 Computer L & Security Rev 99 at 109.

previous sections. There are compelling reasons why privacy standards in relation to parties should have different content than those in other contexts that apply to commercial or government entities. Parties have a unique role in the constitutional, electoral, and democratic order. Their particular role, however, does not displace the risk that self-regulation will lead to under-protection of privacy, because stringent privacy standards would be at odds with the short-term interests of parties. For example, mandatory disclosure of a data breach by a party would expose them to critique and could even harm their electoral prospects if the resulting harm was wide-spread and egregious enough. Rules on data collection, to take another example, might restrict the information that ultimately ends up with parties, and therefore hinder their attempts at micro-targeted voter communications. Ensuring that voter privacy is protected would also cost parties money and resources in additional labour and technical infrastructure, compounded by the lack of continuity in staffing and the rapid and large spikes in temporary personnel during campaigns.

Parties could adopt the view that voter privacy is important as a matter of principle or that their long-term interests are better served by the trust that could be generated if voters have faith that their personal information, if acquired, will not be unduly harvested or misused. There is a large literature in Canada, however, on how narrow interpretations of a party's own partisan and electoral self-interest often shape the decisions of governments around electoral legislation.[141] There is no reason to assume that voter privacy would somehow escape the partisan lenses that shape the laws regulating elections more generally.

It could be countered that parties should be left as unregulated as possible as a general matter so that the state does not interfere in their internal workings, and that this principle suggests that the government could nudge parties to protect voter privacy but should not impose hard regulations.[142] However, this hands-off approach of self-regulation coupled with rhetorical support for

141. See Heather MacIvor, "Do Canadian Political Parties Form a Cartel?" (1996) 29 Can J Pol Sci 317; Colin Feasby, "Freedom of Expression and the Law of the Democratic Process" (2005) 29 SCLR (2d) 237; Michael Pal, "Breakdowns in the Democratic Process and the Law of Canadian Democracy" (2011) 57 McGill LJ 299 at 319-21; Yasmin Dawood, "Electoral Fairness and the Law of Democracy: A Structural Rights Approach to Judicial Review" (2012) 62 UTLJ 499.

142. See Richard H Thaler & Cass R Sunstein, *Nudge: Improving Decisions about Health, Wealth, and Happiness* (Yale University Press, 2008) (drawing on behavioural economics for a "libertarian paternalism" approach in which government provides choice architecture to nudge people toward decisions preferred by the government without mandating conduct through hard law).

privacy protections effectively exists now and has fallen short. Parties have not been vigilant in protecting voter privacy and have not voluntarily refrained from adopting practices and technologies that pose serious privacy risks to voters, including big data analytics and reliance on data brokers. The parties' incentives in favour of data collection have been exacerbated by the low cost of data storage. Self-regulation has been tried and has been insufficient to protect voter privacy.

Elections Canada and the BC Information and Privacy Commissioner have suggested implementing a voluntary code of conduct for political parties, including protections for personal information.[143] The advantages of a voluntary code are to provide more persuasive power to regulators, increase public trust in parties, encourage the parties to coalesce around common practices, remind parties of their duties to the public, support party members with ethical concerns, and to be consistent with other sectors that have implemented codes of ethics.[144] Elections Canada's 2020 discussion paper on voter privacy observed that a "voluntary code may be more palatable to political parties than legislated change, while at the same time moving towards increasing electors' privacy."[145] However, a voluntary code of conduct would be susceptible to the same problems that have afflicted the current self-regulatory approach where, in the absence of a statutory mandate, the incentives for parties have been in favour of collecting more information about voters to obtain an electoral advantage. A voluntary code might simply reiterate the statutory obligations that already exist, on the one hand, or be too vague or general to provide practical guidance, on the other hand.[146] In the absence of statutory requirements to protect voter privacy, coupled

143. Elections Canada, "A Code of Ethics or Code of Conduct for Political Parties as a Potential Tool to Strengthen Electoral Democracy in Canada" (2018), online: <www.elections.ca/content.aspx?section=res&dir=rec/tech/cod&document=table&lang=e> [EC, "Code of Ethics"].
144. McEvoy, *Full Disclosure*, *supra* note 5 at 43-44.
145. Elections Canada, *Political Communications in the Digital Age, Discussion Paper 3: The Protection of Electors' Personal Information in the Federal Electoral Context* (May 2020) at 17, online: <www.elections.ca/res/cons/dis/compol/dis3/dis3_e.pdf>.
146. See EC, "Code of Ethics," *supra* note 143. Indeed, it is suggestive that *PIPEDA*, which has been criticized as a "creature of compromise" attributable to its original drafting style, is itself a result of codifying a model code that originated as a self-regulatory scheme for business. ISEDC, *supra* note 128, at Part 4.

with enforcement powers to secure compliance, the parties are unlikely to effect strong change on their own.[147]

2. CONTINUOUS APPLICATION OF PRIVACY OBLIGATIONS

Second, privacy protections should apply continuously, rather than being time limited or tied to an electoral event, to align with the full-year and years-long campaign strategies of political parties. Rules limited to specific election periods have been problematic in other contexts. For example, the rules limiting spending by political parties and third parties are restricted to the official campaign period, beginning with the drawing up of the writ and ending on election day. The *EMA* introduced a slightly longer period in which spending is regulated, by imposing a pre-writ spending limit that begins on June 30 of an election year in the lead up to the fixed date vote in October.[148] These time-based restrictions create an obvious loophole, as political and third parties have incentives to advertise in the unregulated period where no spending limit applies.[149] Another factor is the lack of continuity in political parties' staff. During campaigns, parties see rapid influxes of temporary personnel who often have access to troves of voter information without adequate privacy training to protect it.[150] To avoid creating any gaps in privacy protection, any privacy rules that apply to parties should apply at all times, and not simply during the official election campaign or the immediate pre-writ period. The counter argument against continuous restrictions on spending limits is primarily a constitutional one. As spending on advertising is covered by the *Canadian Charter of Rights and Freedoms*' ("*Charter*") guarantee of free political expression in section 2(b), restrictions over a longer time frame are

147. If Canada were to implement a statutory code, oversight could be placed either with the Commissioner of Canada Elections, who is located in the Office of the Director of Public Prosecutions, or with Elections Canada since the 2014 changes in the *FEA.* See *FEA*, *supra* note 30; EC, "Code of Ethics," *supra* note 143. The UK ICO recommended a statutory code of conduct. See ICO, *Democracy Disrupted*, *supra* note 3, at 44. The ICO has since issued a draft framework for a code of conduct. See United Kingdom, Information Commissioner's Office, *Guidance on Political Campaigning: Draft Framework Code for Consultation* (2019), online (pdf): <ico.org.uk/media/about-the-ico/consultations/2615563/guidance-on-political-campaigning-draft-framework-code-for-consultation.pdf>.

148. *EMA*, *supra* note 13, s 349.1.

149. Pal, "Is the Permanent Campaign the End of the Egalitarian Model of Elections?," *supra* note 8.

150. See McEvoy, *Full Disclosure*, *supra* note 5 at 29 (recommending that political parties in BC provide employee and volunteer training plans and materials before they can receive the voter lists).

more harmful to individual rights holders.[151] But this has to be weighed against the right to privacy and democratic principles.

3. PROTECT INDIVIDUAL VOTERS RATHER THAN "VOTER DATA"

Third, legislation to protect voter privacy should focus on protecting the privacy of voters and not simply protecting the category of "voter data." Data about individuals does not fit neatly into boxes. It may be characterised as "voter data" when political parties use it for political purposes such as determining the persuadability of voters; however, the same data deployed for a different purpose by a different actor may be characterised as "consumer data" or "advertising data." With big data analytics, what political parties do is hard to differentiate from what commercial actors do and is often based on commercial approaches. Both are interested in commercial data, both draw inferences about preferences, and both develop psychographic profiles about individuals. Political parties do this to gauge the likelihood of voting and persuadability; commercial actors do so to gauge the likelihood of buying and product preferences. Given the ubiquity, fluidity, and variety of data, and the proclivity of political parties for extrapolating political preferences from non-political data, it would be difficult to administer a system that sharply differentiates between players in the data ecosystem, and it would be difficult to provide effective privacy protection for voters in such a segmented system. With the multitude of layers, actors, technologies, and data sources involved, an effective regulatory measure should not depend on legislative distinctions that are hard to administer. It should not differentiate between "voter data" and other categories of data, between data from "political" sources and non-political sources, or between data drawn from "political" activities and other activities.[152] Recognizing a separate category of "voter data" or a separate category of "political" sources in the law would be at odds with how data ecosystems actually operate in practice and the multiple channels of information drawn upon by parties.

One could argue that if voter data cannot be disentangled from other data, why not simply include political parties under *PIPEDA* along with commercial entities? *PIPEDA*, as currently constituted, is inadequate for the regulation of personal information and commercial entities, as detailed above, in Part II.A., and would likewise provide insufficient protection if it were to regulate voter

151. Part 1 of the *Constitution Act*, 1982, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11, s 2(b).

152. See Roger A Ford, "Unilateral Invasion of Privacy" Notre Dame L Rev 1075 at 1083 (on the difficulty of differentiating types of data). See Delacourt, *supra* note 37.

data and political parties. While voter data is hard to differentiate from other personal information, in our view it would be difficult or perhaps even impossible to adequately accommodate the context of political parties even in a reformed *PIPEDA*. The relationship between political parties and voters is of a different kind than that between commercial entities and consumers. The balance required to facilitate communication between parties and voters so as to respect the foundational importance of that relationship in a democracy, while respecting legitimate privacy concerns, is difficult enough to achieve on its own, as the failure to do so to date in Canadian legislation demonstrates. Striking that balance between facilitating democracy and upholding privacy would not be possible if other concerns related to commercial entities and relationships were added to the mix and if the legal mechanism to carry out that effort was hampered by *PIPEDA*'s flaws.

4. TECHNOLOGICAL NEUTRALITY AND FUTURE-FOCUSED REGULATION

Fourth, Canada should adopt a technologically neutral approach in its regulation. Protection for voter privacy would be undermined by even the best possible legislative response if the reforms were explicitly tied to existing technologies for collecting and analysing personal information. Technology and, as a result, political campaigning, are rapidly evolving. Legislative protection for voter privacy will be more effective if it is neutral with regard to the technology being used. In other words, it should be broad enough to apply even to new technologies that will inevitably develop, and which will, equally inevitably, be deployed by campaigns and thus have an impact on voter privacy.

The importance of technological neutrality has been emphasised in related areas of the law. The Supreme Court of Canada has supported the principle of technological neutrality in various contexts whereby, unless there is Parliamentary intent to the contrary, the statute "should not be interpreted or applied to favour or discriminate against any particular form of technology," and the statute's traditional balance "must be maintained across all technological contexts" and "should be preserved in the digital environment."[153] Applying this principle, voter privacy legislation should not attempt to specify the types of technology

153. *Canadian Broadcasting Corp v SODRAC 2003 Inc*, 2015 SCC 57 at paras 66-68.

that are used to collect data, nor the methods that are used to analyse that data.[154] As media and devices can change with different technologies, the legislation should not be locked into a particular format, process, or source.

It is possible that, by being too general and abstract, privacy-focused reforms might undermine their long-term effectiveness, as the particular details of technologies or their uses matter. However, legislation crafted too specifically around a particular technology is vulnerable to being outdated quickly. Similarly, legislation designed around particular platforms or business models may be too restricted and may make it difficult for all affected companies to comply. For example, amendments introducing a requirement that social media platforms maintain registries of political advertisements communicated on their sites were heavily critiqued by some of the platforms for being designed around the technical specifics of Facebook. Google, for instance, claimed that it was impossible for them to comply with the new requirements, given how advertisements were placed on their sites.[155] Care should thus be taken to ensure that the intended subjects of the regulatory regime are able to comply. The saga around the advertising registry is a cautionary tale. Without technological neutrality, reforms may not achieve the desired objective because they are too narrowly focused and, even if effective, may quickly be obsolete because of technological developments. It is important to note that even statutes designed to be technologically neutral, such as *PIPEDA*, still reflect the concerns and practices made possible by the technologies of their time,[156] and thus the need for amendments for even a well-crafted statute will be foreseeable at some future horizon. However, that time period can be lengthened

154. For example, although Europe's modernization efforts to update privacy law to incorporate automated processes are laudable, there are already critiques that the *General Data Protection Regulation (GDPR)* is not forward thinking enough in its language around the technologies. See EC, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* [2016] OJ 679/2016 [*GDPR*]. See Karen McCullagh, "The General Data Protection Regulation: A Partial Success for Children on Social Network Sites?" in Tobias Bräutigam & Samuli Miettinen, eds, *Data Protection, Privacy and European Regulation in the Digital Age* (Unigrafia, 2016) 110 at 122, 127-29; Michael Butterworth, "The ICO and Artificial Intelligence: The Role of Fairness in the GDPR Framework" (2018) 34 Computer L & Sec Rev 257 at 265; Jenna Lindqvist, "New Challenges to Personal Data Processing Agreements: is the GDPR Fit to Deal with Contract, Accountability and Liability in a World of the Internet of Things?" (2018) 26 Intl JL & IT 45 at 61-63.

155. See Tom Cardoso, "Google to Ban Political Ads Ahead of Federal Election, Citing New Transparency Rules" (4 March 2019), online: *The Globe and Mail* <www.theglobeandmail.com/politics/article-google-to-ban-political-ads-ahead-of-federal-election-citing-new>.

156. See ISEDC, *supra* note 128 at Part A: Possible Options—Consent and Transparency.

by a commitment to technological neutrality in the design of the statutory framework. Technological neutrality remains an essential aspect of any reform likely to be meaningful in the long term.

5. LIMIT DATA USE TO POLITICAL PURPOSES ONLY AND PROHIBIT COMMERCIAL ACTIVITIES

Fifth, the uses to which political parties can put voter data must be strictly tied to their role in democracy. Parties should be permitted to use voter data only for "political purposes," meaning non-commercial activities. Parties play a key role in democracy, but they are in a relatively privileged position. Even though the direct *per* vote subsidy, which gave parties quarterly funding based on their vote totals from the previous election, was eliminated, parties receive significant indirect public financial support. The contributions that sustain their activities are subject to generous tax rebates, far exceeding those in the charitable sector.[157] Parties and their candidates also receive significant reimbursement of the expenses that they incur to contest elections.[158] Registered parties have a variety of statutory and even constitutional protections.[159] This preferential treatment can be justified on the basis that healthy parties are required for electoral democracy to function. But permitting parties to use data for non-political purposes would unduly permit them to use these financial benefits and rights outside of the realm of electoral politics. This would be contrary to the reason for those benefits and rights being conferred, which was strictly to have robust democratic competition for votes and seats.

It is true that the definition of a "political party" in section 2 of the *CEA* only requires that "one of [its] fundamental purposes is to participate in public affairs by endorsing one or more of its members as candidates and supporting their election."[160] One could interpret the definition not only to permit, but even to anticipate, that parties would engage in non-political purposes. The more persuasive reading of the definition, however, is that parties might engage in activities other than endorsing candidates, such as fundraising, expressing

157. See *Income Tax Act,* RSC 1985, c 1 (5th Supp), s 127(3).
158. See Elections Canada, "Total Paid Election Expenses and Reimbursements, by Registered Political Party – 2015 General Election" (12 May 2020), online: <www.elections.ca/content.aspx?section=fin&dir=oth/pol/remb&document=table1_15&lang=e> (for the most recent publicly available reimbursement data).
159. See *e.g. Figueroa*, *supra* note 11. There, the Supreme Court found that onerous rules depriving small political parties of the benefits conferred by registration were unconstitutional for violating section 3 of the *Charter*.
160. *CEA*, *supra* note 8.

political views, advertising, and so on. Although these activities might not always be directly related to electing candidates, these other purposes for its behaviour are assumed to be political rather than, say, religious or commercial or some other shared purpose that the members might pursue.

Any discussion of potential commercial activities by parties raises the issue of whether they should be allowed to sell valuable commodities that they hold, such as voter data. Political parties should *not* be permitted to sell voter data to other entities or transfer it to any entity seeking to use this information for commercial gain. This rule is appropriate for several reasons. If parties were permitted to sell voter data, individuals would likely be reluctant to provide information to parties, which would hamper democracy more generally. Few individuals would anticipate that indicating their voting preferences to a door-to-door canvasser, "liking" a photo of a leader's newborn baby, or sharing a photo of a candidate would mean their information is transmitted for a price to a commercial entity seeking to sell rafting tours, children's clothes, or movie tickets.

It is not clear what public policy rationale would exist for continuing to permit political parties to sell the data they have collected about voters to non-political entities. Perhaps it could be justified as a necessary evil to provide the funds parties need to operate. The generous, though indirect, public funds available to parties undermine the strength of any such claim. Selling data provides money to the parties but without improving parties' ability to communicate with voters, and it further hampers voter privacy.

The *EMA* merely requires that parties *disclose* their policy with regard to selling data and does not restrict the practice. In doing so, it advances voter privacy incrementally, without addressing the fundamental issue that the sale of voter data by parties is harmful to democratic participation. Rather than permitting parties to sell voter data only if individuals consent, we instead recommend establishing a general rule that political parties are permitted to use personal information only for political purposes and are banned from any commercial activity with respect to voter data. Limiting the use of personal data to the purposes for which it was collected is an established fair information principle,[161] and the only defensible use that political parties should make of data are those related to the parties' political purpose.

---

161. See *PIPEDA*, *supra* note 7, Schedule 1, s 4.5, Principle 5 (stating "[u]nless the individual consents otherwise or it is required by law, personal information can only be used or disclosed for the purposes for which it was collected.").

6. INFORMED CONSENT

Sixth, parties should be required to comply with the principle of informed consent for all uses of personal data for political purposes. Consent is intended to support autonomy by allowing individuals to choose what happens with their personal information. Although consent is a central mechanism for data protection legislation, it has not been effective in providing individuals with real control or decision-making over their data. The OPC's 2019 Guidelines for Obtaining Meaningful Consent remarks that "advances in technology and the use of lengthy, legalistic privacy policies have too often served to make the control – and personal autonomy – that should be enabled by consent nothing more than illusory."[162]

This "illusion" of control is particularly salient for voters, who lack enough information and enough alternatives to make consent meaningful in the context of big data analytics by political parties.[163] The information asymmetry endemic to big data practices makes it increasingly difficult for individuals to know what information parties have about them and how it is being used by parties. It is also hard for voters to know what other entities have access to the data and where it goes in their hands and to exercise meaningful choice about those downstream uses. The lack of accountability in parties' data practices will not improve much with the 2018 elections law amendments, which require basic disclosures of certain data activities but not voter consent. The *EMA* only requires parties to disclose "the party's practices concerning…the collection and use of personal information created from online activity."[164] But it imposes no obligation that the parties obtain voters' consent for these data practices.

---

162. Office of the Privacy Commissioner of Canada, *Guidelines for Obtaining Meaningful Consent* (24 May 2018), online: <www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805> [OPC, *Guidelines for Obtaining Meaningful Consent*]. See also, Office of the Privacy Commissioner of Canada, "Consent" (2019), online: <www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent>; Office of the Privacy Commissioner of Canada, "Submissions Received for the Consultation on Consent" (2016), online: <www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-on-consent-under-pipeda/submissions-received-for-the-consultation-on-consent>.
163. See Digital, Culture, Media and Sport Committee, *Disinformation and 'Fake News' Interim Report*, *supra* note 5, at para 75 (noting that social media companies "give users the illusion of users having freedom over how they control their data, but they make it extremely difficult, in practice, for users to protect their data"). For the final report, see UK, Digital, Culture, Media and Sport Committee, *Disinformation and 'Fake News': Final Report*, Eighth Report of Session 2017-19 (Cm 1791, 2019).
164. *EMA*, *supra* note 13, s 254(1)(v)(A).

The practices for obtaining consent by the private sector are continuing to develop, as showcased in the ETHI Committee's report on updating *PIPEDA* and in the OPC's Guidelines for Obtaining Meaningful Consent.[165] Those reports continue to support individual consent as a viable regulatory mechanism and suggest ways to strengthen it. The OPC principles emphasize that consent is "an ongoing process that changes as circumstances change" and should be treated as "a dynamic and interactive process."[166] The intrusiveness of big data practices should require more stringent consent.

We recommend that informed consent obligations apply to political parties. Political parties should be required to obtain voters' explicit consent and respond to the privacy preferences that individuals hold. The applicable regulatory agency should develop an informed consent policy, to which parties are required to adhere, for in-person and online interactions with voters and also with respect to the parties' acquisition and analysis of voter data. Informed consent would require that political parties provide individuals with information in a user-friendly form about what data is being collected, how it is being collected, and whom it is being shared with, and that individuals explicitly agree to the specific use of their data.[167] The policy should set out explicit threshold requirements for parties setting out how and when parties must obtain consent, the data activities that require consent, and the parties' confidentiality obligations with respect to the data. The responsible agency should periodically review the template informed consent policy to update it for technology changes that affect voter privacy. Political parties should generally be required to obtain informed consent for any personal information, including inferences pertaining to individuals, such as persuadability scores. Inferences about individuals should be treated as personal information regardless of whether the inferences are accurate or predictive.[168]

---

165. ETHI, *Towards Privacy by Design*, *supra* note 5 at 25-28; OPC, *Guidelines for Obtaining Meaningful Consent*, *supra* note 162.
166. OPC, *Guidelines for Obtaining Meaningful Consent*, *supra* note 162.
167. *PIPEDA*, *supra* note 7, s 6.1 (which provides one version). See also *Ontario Personal Health Information Protection Act*, *2004,* SO 2004, c 3, Schedule A, s 18(5) (defining "knowledgeable consent" as "if it is reasonable in the circumstances to believe that the individual knows, (a) the purposes of the collection, use or disclosure, as the case may be; and (b) that the individual may give or withhold consent").
168. See Digital, Culture, Media and Sport Committee (UK), *Disinformation and 'Fake News': Final Report*, *supra* note 163 at para 48 (supporting ICO's recommendation that "inferred data should be as protected under the law as personal information" and recommending that the UK Government study how "the protections of privacy law can be expanded to include models that are used to make inferences about individuals, in particular during political campaigning").

Incorrect inferences may still have an impact on the individual about whom the inference was made and should therefore be included as personal information. For example, a party may wrongly infer that voters with certain movie or vacation preferences are unpersuadable for their party, causing a party's candidates not to contact those voters.

Political parties should also be responsible for ensuring that consent was obtained throughout the "data chain" and that all relevant parties obtained explicit consent for any data to be used for a political purpose.[169] Parties should be ultimately responsible for ensuring that informed consent has been obtained for all data, and should not rely on statements about consent made by third parties such as databrokers and social media platforms.[170] Political parties should be responsible for the campaign-related activities of their associated databrokers and for any downstream uses of voter information. Similarly, individuals may consent only to the use of their own information, and not information about other people. Political parties must seek consent from the voter and not piggyback off the consent of an individual who allows access to their contacts.

Voters should not have the burden of trying to trace where all the data has come from and whether they consented at each step. In the context of algorithmic processes, it is difficult for voters to know what data is being used for what purpose and what assumptions underlie the inferences being made.[171] As political inferences are made from an amalgamation of data that may have little to do explicitly with politics, voters will have difficulty detecting that their data is being used for this purpose. Relatedly, the volume and complexity of these data transactions makes it difficult for government regulators to monitor consent and impose effective accountability measures on campaigns. Hence, the burden should be on political parties to demonstrate informed consent by individual voters for all data. Parties should be required to keep records documenting

169. The UK Information Commissioner's Office similarly recommends that political parties apply "due diligence when sourcing personal information from third party organizations, including data brokers, to ensure the appropriate consent has been sought from the individuals concerned." ICO, *Democracy Disrupted*, *supra* note 3 at 5.

170. See similarly *ibid*, at 51 (noting that "[w]e do not believe that insertion of simple contractual terms between [a political party] and a data broker is sufficient to mitigate the risk").

171. Rob Kitchin describes three challenges to researching algorithms: obstacles to gaining access to their formulation; algorithms are heterogeneous and embedded in wider systems; and their work unfolds contextually and contingently. Rob Kitchin, "Thinking Critically About and Researching Algorithms," (2017) 20 Info Comm & Soc'y 14. These obstacles would also hinder transparency and accountability with respect to campaign algorithms. They are suggestive of the difficulties that would likely be encountered by regulators trying to monitor algorithms and individuals trying to protect their data.

consent for all data, and these records should be subject to audits in the same way that records of party finances are.

7. EXPAND OPT-OUT TO COVER ANY PERSONAL INFORMATION HELD BY POLITICAL PARTIES

Seventh, voters should have the ability to opt out of any collection and use by political parties of their personal information. In other contexts, as detailed in Part II, many contacts between political parties and voters are regulated.[172] Under these existing rules, voters have some ability to control their contact with political parties. Voters already have the right to opt out from the Register and to request to be on a party's internal do-not-call list. Other aspects of unsolicited contacts by political parties are also regulated. The CRTC regulates unsolicited calls during federal elections and has identified "[p]rotecting citizens' right to privacy" as an objective for these rules.[173]

Extrapolating from these rules, voters should be able to have greater control over whether and how their data is collected and used by political parties. To update the existing voter contact rules and provide similar privacy control in the big data context, voters should be able to opt out of their information being included in political parties' databases. We recommend that political parties be prohibited from collecting or using personal information about any voter who has opted out of the Registry unless they provide explicit consent for these other data uses.

We also recommend that the CEO should undertake educational efforts to notify voters of their opt-out options. Currently, there is a check-off box on individual income tax forms that people can select to opt out of the Canada Revenue Agency sharing their information with Elections Canada to update the Register. The CEO could additionally coordinate the process by which voters may opt out from political parties' databases. To increase transparency and accountability around political parties' data practices, the CEO should educate voters about how political parties use their personal information, the voters' rights with respect to their data, and their options to opt out of political party databases. Material informing voters of their ability to opt out from the electoral Register, as well as from political party databases, could be included on mailed voter cards and on prominent notices at polling stations.

---

172. CRTC, "Rules for Unsolicited Telecommunications Made on Behalf of Political Entities," *supra* note 97.
173. CRTC, "Protecting You from Rogue and Misleading Calls During Federal Elections," *supra* note 104.

One concern might be that, if individuals are able to pre-emptively and generally opt-out of contact from political parties, there would be a reduction in the number of Canadians that parties could contact to solicit their views, votes, and financial contributions. But in practice, few voters have opted out of the Register.[174] Political parties and candidates may continue to use the list of electors to communicate with voters who have not exercised their opt out, including for the purposes of soliciting contributions and recruiting party members. Political parties could continue to use non-identifiable personal information to formulate public policy and to use personally identifiable information of voters who consent.

8. ADDITIONAL VOTER RIGHTS PERTAINING TO BIG DATA ANALYTICS

Eighth, beyond fair information principles, voters should have additional rights to address big data. Neither federal nor provincial privacy legislation adequately considers the impact of big data and predictive analytics. *PIPEDA* has not been amended yet to incorporate the new challenges of big data analytics, nor have the other major privacy statutes in Canada. The European Union's *General Data Protection Regulation* (*GDPR*), which came into force in 2018, updates the EU *Privacy Directive* by addressing automated processing of data.[175] The *GDPR* confronts the challenges of big data by, inter alia, increasing transparency obligations,[176] regulating algorithmic decision making by enforcing a right to an explanation,[177] emphasizing consent,[178] and placing increased responsibilities on data controllers through the right to erasure[179] and the right to de-index.[180] Under the *GDPR*, political opinion is part of the regulation's definition of "sensitive

174. In a June 2019 report, Elections Canada reports that there are 26.1 million electors on the Register, and since 1997, there have been 4200 opt outs from the Register and 160 requests to opt out from sharing data with other jurisdictions. Elections Canada, *National Register of Electors—Updates: June 2019 Annual Lists*, Report (Elections Canada, June 2019).
175. EC, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,* [1995] OJ L 281/31. See also Barbara McIsaac, Rick Shields & Kris Klein, *The Law of Privacy in Canada*, Student ed (Carswell, 2004); Colin J Bennett, "Voter Databases, Micro-targeting, and Data Protection Law: Can Political Parties Campaign in Europe as they do in North America?" (2016) 6 Intl Data Privacy L 261 at 267.
176. *GDPR*, *supra* note 154, art 12.
177. *Ibid*, art 22. See also Bryce Goodman and Seth Flaxman, "European Union Regulations on Algorithmic Decision-Making and a 'Right to Explanation'" (Fall 2017) *AI Magazine* 50.
178. *GDPR*, *supra* note 154, art 7.
179. *Ibid*, art 17.
180. *Ibid*, art 18.

form of personal data."[181] Recital 56 of the *GDPR* permits political parties to compile data on political opinion, but parties' data practices remain subject to the *GDPR*.[182] The European Commission has provided guidance for various election-related actors on *GDPR*'s data protection rules, which advise parties and data analytics companies not to process personal data that was provided for a purpose unrelated to the election and advise social media companies not to share data with other companies without explicit consent.[183] In the Parliamentary report by Canada's Standing Committee on Access to Information, Privacy and Ethics,[184] the committee recommended that Canadian privacy legislation place greater emphasis on big data problems[185] and made several recommendations that borrow from the *GDPR*.[186]

We recommend incorporating rights to increase transparency and accountability about parties' use of big data and analytics. Individuals should have a right to know specifics about what information political parties hold about them and where it was obtained. Voters should also have a right to correct the data if it is inaccurate. More controversial among the GDPR rights would be to grant voters a right of explanation, which would provide voters with a right to know the reasons for algorithmic decisions made about their voting preferences

181. *Ibid*, art 9(1).
182. *Ibid*, art 9(2), Recital 56 (stating that, in the course of electoral activities, where the operation of the democratic system requires in certain Member States that political parties compile data on people's political opinion, the processing of such data may be permitted for reasons of important public interest, provided that appropriate safeguards are established). Parties must still comply with *GDPR* provisions pertaining to data protection, access requests, consent, data retention, data minimization, and deletion. See ICO, *Democracy Disrupted*, *supra* note 3 at 19 (with reference to the *GDPR*, "political parties are not exempt from data protection law; they have responsibilities as data controllers to comply with all the requirements of the law, including the data protection principles"); UK, Information Commissioner's Office, *Guidance on Political Campaigning*, vol 3.1 (ICO: 28 March 2018) (updated guidance for parties on application of *GDPR* to political campaigns).
183. European Commission, "Protecting Europeans' Personal Data in Elections" (12 September 2018), online (pdf): <ec.europa.eu/commission/sites/beta-political/files/soteu2018-factsheet-personal-data-elections_en.pdf>.
184. ETHI, *Towards Privacy by Design*, *supra* note 5.
185. *Ibid* at 23.
186. For example, Recommendation 3: algorithmic transparency, Recommendation 11: right to erasure, Recommendation 12: right to de-indexing, Recommendation 13: destruction of personal information. *Ibid* at 25, 43-50.

and persuadability, and a right to erase data.[187] By comparison, *PIPEDA*'s fair information principles include having accurate and complete data, and having access to data in order to challenge its accuracy and completeness and have it amended.[188] However, there is neither a right to erase data nor a right to explanation in *PIPEDA*.

On the one hand, a right to erase information could frustrate the function of political parties in interacting with voters before and during election time. On the other hand, voter autonomy and informed consent would support voters being able have their data removed if they no longer want to be included, or never consented to being included, in a party's database. A right to erase would be consistent with other options Canadian voters have, including opt-outs for the national Register and requesting to be placed on a party's internal do-not-call list. A right to erase could be seen as effectuating and updating these existing voter rights by providing similar mechanisms for voters to exercise their data preferences in the context of big data.

We endorse a compromise position that parties would be obliged to destroy some data at the request of the voter, such as that obtained through big data inferences, while being permitted to keep the basic data to which they are entitled from the Register (provided the voter did not opt out) or to retain some other minimally intrusive subset of data. Parties should also be permitted to retain data that was volunteered by voters through direct interactions with parties or candidates, such as during canvassing. Claims from parties that they are entitled to keep basic information needed to communicate with the electorate and information that they have obtained through direct voter interactions are more compelling than claims that political parties are entitled to keep data that has been acquired from a commercial entity, data that includes non-political information, or psychological inferences drawn from such data, when the individual wants it to be destroyed. We also support a limited data retention period of ten years, as described below in Part III.D.10.

Finally, at this time we do not recommend that voters have a right to know what political decisions political parties have made about them on the basis of big data. We believe that a right to explanation would impinge on campaign

187. See *GDPR*, *supra* note 154, art 15, art 17, and Recital 71. The *GDPR*'s most explicit description of the right of explanation is in Recital 71, which is non-binding. Recital 71 provides that decisions based solely on automated processing and producing a legal effect that significantly affect a data subject should have suitable safeguards, including specific information to the data subject and the right to human intervention to obtain an explanation of the decision and to challenge it.

188. *PIPEDA*, *supra* note 7, Schedule 1, ss 4.6, 4.9, Principles 6 and 9.

strategies and party policies. We therefore do not recommend a *GDPR*-style right to an explanation, but it is an option that is likely to be considered.

9. DATA SHARING

Ninth, in addition to political parties being barred from using data for non-political purposes, which would preclude parties from selling information to commercial actors, political parties should be regulated in how they share voter information. We recommend three rules for data sharing with third parties, data sharing with other parties, and data sharing within a party.

I. DATA SHARING—THIRD PARTIES

Political parties should be prevented from sharing voter information with third parties. Third parties are broadly defined in section 349 of the *CEA* to include any entities or individuals other than political parties, candidates, leadership contestants, nomination contestants, and electoral district associations. Political advertising by third parties is heavily regulated by the *CEA*. Third parties are required to register spending over $500 on political advertising, to disclose information on their structure and activities to Elections Canada, and to abide by a spending limit for advertising during the election period.[189] Political parties and third parties are distinct legal entities and must operate at arm's length.[190] Political parties are legally barred from colluding in a variety of ways with third parties.[191] The collusion rules in the *Elections Act*, which are designed to prevent attempts to evade the rules on political advertising, impose mandatory registration of third parties, require disclosure about the entity purchasing the advertising, and establish financial spending limits for both political parties and third parties.[192]

The same type of collusion rules that apply to political advertising should apply to data. Collusion between political parties and third parties on voter data is as troubling as collusion between political parties and third parties on advertising. Any type of collusion between the entities harms electoral integrity.

---

189. *CEA*, *supra* note 8, s 353(1).
190. See *CEA, supra* note 8, s. 349, where the definition of "third party" excludes registered political parties and their candidates and electoral district associations.
191. See Michael Pal, "Third Party Political Participation and Anti-Collusion Rules" (2018) 61 Can Pub Admin 284.
192. See Elections Canada, "Interacting with Third Parties in the Pre-election and Election Periods" in *Political Financing Handbook for Registered Parties and Chief Agents* (April 2020), ch 11.

Collusion between political parties and third parties around voter data has the added dimension of potentially harming voter privacy.

Such rules prohibiting data collusion would limit the flow of information between political parties and third parties. There would be minimal—if any—harms resulting from such reforms. Any significant exchange of information that leads to coordination around advertising, for example, is already barred, since they are distinct legal entities that must operate at arm's length. The same reasoning applies to collusion about data that emerges from, for example, sharing information about voters. Permitting data collusion would undermine the effectiveness of the existing anti-collusion provisions in the *CEA*, which are focused on preventing avoidance of spending and contribution limits.

II. DATA SHARING—OTHER POLITICAL PARTIES

Data sharing between political parties in Canada is less problematic than sharing with third parties and should be permitted, provided there is informed consent by the voter. Data sharing between different Canadian political parties would arise if federal political parties want to formally divulge their voter information with their official provincial affiliates or the candidates for leadership of the party. Federal political parties might also wish to share the data informally with technically unaffiliated (but, in practice, politically allied) provincial parties, or even municipal candidates. In contrast to data transfers involving political parties and commercial entities, the data transfers between Canadian political parties involve entities that all have political purposes. In contrast to data sharing between political parties and third parties, the data sharing between Canadian political parties involves entities that operate in different election jurisdictions, which eliminates the concern about collusion that attaches to sharing with third parties.

Given these differences, a key issue that remains is voter consent for these downstream uses of voter data. To satisfy informed consent, the privacy rules applying to the data held by these other political parties should be clearly described. Voters should be able to get information when requested about data sharing and the privacy protections in place to protect their data in the hands of the transferee. It is possible that local or provincial rules are so diverse that there will be unsatisfactory privacy protection for the shared data when it reaches new hands. One option is that a party could share data with a second party

in another jurisdiction only where that jurisdiction has "substantially similar" privacy protections to those that would be operating at the federal level.[193]

III. DATA SHARING—WITHIN THE SAME PARTY

Information sharing within parties should largely be facilitated, provided that voter data is treated confidentially and appropriate security measures are taken, as discussed in Part III.D.10. As long as it is necessary for political activities, sharing information between the central party and its candidate in a riding or the electoral district association (EDA) should be permitted if reasonably related to the purposes for which a voter originally consented. Preventing the flow of information between affiliated entities would fly in the face of how parties operate, which is increasingly as centralised organizations.[194] Such information may be particularly useful for campaigning or fundraising. Although under the *CEA* political parties are separate legal entities from candidates, leadership contestants, and EDAs, the *CEA* nonetheless envisions a close relationship between them and already facilitates it in multiple ways, such as permitting the transfer of money or non-monetary resources. Data should be treated the same way as other resources that the *CEA* already allows to be transferred, provided that there is a legitimate political purpose for the internal sharing of data. Parties should be required to have internal controls to make sure that only those authorised to view the data may do so.

10. CYBERSECURITY PROTOCOLS

Tenth, political parties should be required to implement cybersecurity protocols to protect the storage and transmission of voter data by political parties. The

193. A similar condition is in place with *PIPEDA*, where the federal legislation applies unless there is "substantially similar" provincial legislation. See *PIPEDA*, *supra* note 7, s 26(2)(b). This section provides that the Governor in Council can exempt organizations or activities from *PIPEDA*'s application if the province has passed substantially similar legislation. British Columbia, Quebec, and Alberta have their own provincial private-sector privacy legislation. See *Personal Information Protection Act*, SA 2003, c P-6.5; *Personal Information Protection Act*, SBC 2003, c 63; *Act Respecting the Protection of Personal Information in the Private Sector*, CQLR c P-39.1. Additionally, Ontario, New Brunswick, Nova Scotia, and Newfoundland have their own health privacy legislation. See *Personal Health Information Protection Act*, 2004, SO 2004, c 3, sched A; *Personal Health Information Privacy and Access Act*, SNB 2009, c P-7.05; *Protection of Personal Health Information*, SNL 2008, c P-7.01; *Personal Health Information Act*, SNS 2010, c 41.

194. See William Cross & Lisa Young, "Candidate Recruitment in Canada" in Amanda Bittner & Royce Koop, eds, *Parties, Elections, and the Future of Canadian Politics* (UBC Press, 2013) 24 at 25-26. For example, there is central party involvement even in local candidate selection.

unauthorised release of voter data would have privacy and national security implications. The unauthorised release of voters' personal information can lead to identity theft, foreign surveillance, and foreign interference in elections. Political parties are data-rich targets for foreign actors, as evidenced by the hacking of the Democratic National Committee in the 2016 US presidential election.[195] The Communications Security Establishment of Canada (CSE)[196] and Canadian Security Intelligence Service (CSIS)[197] have both identified Canadian political parties as likely targets for foreign interference. The CEO in 2013 recommended amendments to the *CEA* "to require that political parties demonstrate due diligence when giving access to their voter databases."[198] The CEO highlighted the "privacy risks associated with these databases," where political parties "not only handle large amounts of personal information, but also share this information with a small army of volunteers and local campaign workers."[199] The parties' internal management practices matter for how much trust individuals will feel toward parties with regard to their data and are important for electoral integrity.

Parties should be required to adhere to established security protocols for data retention, encryption, and data breach notification. For data retention, we recommend that the maximum amount of time that voter data may be retained should be limited to ten years. A ten-year rule would cover at least two federal elections given the requirement, in section 4(1) of the *Charter*, that elections must be held at least every five years.[200] By comparison, *PIPEDA*'s fair information principles limit the data retention period to only as long as necessary to fulfill

195. The special counsel investigation by Robert Mueller indicted 13 Russian nationals and 3 Russian entities accused of interfering with US elections and political processes. *United States v Internet Research Agency*, *et al*, (16 February 2018) DC Cir, Case 1:18-cr-00032-DLF (Grand Jury Indictment).
196. CSE, *Cyber Threats*, *supra* note 112; CSE, *2019 Update*, *supra* note 112. See generally Elizabeth F Judge & Michael Pal, "Election Cyber Security Challenges for Canada" (2019), online: *Centre for International Governance Innovation* <www.cigionline.org/articles/election-cyber-security-challenges-canada>.
197. See Alex Boutilier, "'Total' Information Warfare a Threat to Democracy: CSIS Report" (22 February 2018), online: *The Toronto Star* <www.thestar.com/news/canada/2018/02/22/csis-says-total-information-warfare-a-threat-to-democracy.html>.
198. CEO, "Preventing Deceptive Communications," *supra* note 137 at 32.
199. *Ibid* at 20.
200. *Charter*, *supra* note 151, s 4(1).

the collection purpose.[201] Applying *PIPEDA*'s purpose guideline could lead to extensive and indefinite retention periods of voter data since "political" purpose could be broadly construed. Shorter retention periods can lessen the impact of a data breach by decreasing the volume of stored data and can reduce the chance of inaccurate outdated data being stored. With the low price of data storage, parties have little economic incentive to delete data on their own initiative.[202] For voters to have predictability about data retention, a fixed term of ten years is preferable. Parties should be required to implement internal security measures to protect voter data (including inferences) such as strong encryption, limiting the number of people who can access the parties' databases, and prohibitions on accessing or storing voter data through unsecured mobile devices or networks. Political parties should be required to notify the CEO of any data breach involving voter data. Political parties should also limit the use of smart devices, such as home assistant devices and other "always-on" devices such as smart speakers, which could record discussions about voter information, resulting in unsecured access. Cloud storage and servers outside of Canada also pose security risks.

11. ENFORCEMENT

Finally, the authority for regulatory oversight of political parties' practices regarding voter privacy should be specifically delineated in the resulting legislation and the available mechanisms for enforcement. *PIPEDA* has been plagued by weak enforcement measures. Under *PIPEDA*, the OPC lacks important powers such as the ability to levy fines and make orders, and individuals can file an action in court only after they file a complaint with the OPC and wait for the Privacy Commissioner's findings to be issued. Under the *EMA*, there are provisions relevant to voter privacy, but their enforcement similarly lacks teeth. The *EMA* requires some reporting in parties' privacy policies about voter data, but it is hard to assess what measures suffice since there are no substantive standards. Further, the enforcement remedy is deregistering, which is a blunt instrument that is unlikely to be applied to a political party.

---

201. *PIPEDA*, *supra* note 7, Schedule 1, s 4.5, Principle 5. See also Élections Québec, *Partis politiques et protection des renseignements personnels: Exposé de la situation québécoise, perspectives comparées et recommandations*, (Report) (Élections Québec, 2019) at 90 (recommending that parties destroy personal information when the use is no longer necessary).
202. See McEvoy, *Full Disclosure*, *supra* note 5 at 31. The BC Information and Privacy Commissioner, in his study of BC political parties, found "all the political parties had an undefined or indefinite retention period for personal information, including information that was incorrect or out of date."

To avoid repeating those enforcement errors, voter privacy legislation should include strong oversight, compliance, and enforcement measures (including audits, inspections, fines, and order making), and it should give individuals a right to bring a cause of action against a political party or campaign directly for privacy infringements.

IV. CONCLUSION

The move toward "big data" politics has serious implications not only for the privacy of Canadian voters but also for the health of democracy and the integrity of elections. As the BC Information and Privacy Commissioner observed,

> robust communication with the electorate is…in the public interest, in the interest of democracy, and not just the political self-interest of the parties. However…this communication should be a fully transparent two-way street. A one sided dialogue in which the public is kept largely in the dark about the significant amounts of personal information collected and used about them is not sustainable legally or ethically.[203]

Nevertheless, the one-way street persists. The current state of legislation in Canada largely exempts political parties from regulation on the collection and use of voters' information, apart from minor obligations in the 2018 amendments to the *CEA* that political parties have a privacy policy. Although there is no certainty that campaigns are running successful or accurate big data practices, concerns over the use—and potential misuse—of voters' personal information arise regardless of the accuracy of the inferences made, given the granularity of voter data in political campaigns, the mass collection of such data, and the manner in which such data is now being used. These big-data practices exacerbate the longstanding problem that political parties have not been regulated by privacy legislation and neither election laws nor other legislation has imposed privacy obligations on parties. So far, Canadian law has not adequately addressed the admittedly complicated interplay of privacy and democratic concerns around voter information in the elections context.[204]

---

203. McEvoy, *Full Disclosure*, *supra* note 5 at 43.

204. After this article was published, the federal government introduced large-scale amendments to *PIPEDA* in Bill C-11. See Bill C-11, *An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts*, 2nd Sess, 43rd Parl (first reading 17 November 2020), online: <parl.ca/DocumentViewer/en/43-2/bill/C-11/first-reading>. However, Bill C-11 does not address the absence of meaningful privacy regulation for political parties as political parties are not subject to the proposed changes to the privacy framework.

Political practices have evolved rapidly over the course of several elections with reliance on big data and microtargeting, and the lack of strong privacy regulation has become more glaring. Data-driven campaigning is here, and here to stay, if we are to judge by the predominance of data-dependent campaigns, the perceived success of data-driven candidates, and the laments by less-than-successful candidates that their fortunes would have been different had there been more and better data about voters. Campaigns, if not voters, seem to be true believers in the value of data. The issues with voter privacy that we have identified in this article are likely to only grow in significance in Canadian politics as new techniques of data analysis relying on more invasive and larger quantities of personal information and new technologies for the more precise analysis of that data emerge, underscoring the need to find solutions to address the gaps in the regulatory framework. It makes little sense that political parties be permitted to operate outside of generally accepted principles of privacy law and best practices for protecting personal information. Political information about voters' beliefs and preferences should be accorded the same protection as the personal information that is held by the private and public sectors about Canadians. Legal reform to protect voter privacy should be done in a manner that respects the personal information of voters and the democratic connection between parties and voters. Toward this end, we have provided eleven guidelines for the design of legislation to protect voter privacy in the age of big-data elections.